Львівський державний університет внутрішніх справ

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Навчальний посібник

Львів
2022

УДК 343.148
С89

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол від 30 червня 2021 р. № 14)

Рецензенти:
***О. А. Губська**, доктор юридичних наук, доцент,
суддя Касаційного адміністративного суду у складі Верховного Суду;*
***А. В. Шевчишен**, доктор юридичних наук, доцент,
начальник відділу розслідування службових злочинів
управління розслідування корупційних злочинів
Головного слідчого управління Національної поліції України*

Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В.
С89 Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.

Узагальнено теоретичну інформацію стосовно об'єктів судової комп'ютерно-технічної експертизи, правил вилучення та зберігання електронної інформації. Визначено завдання, предмет і питання, які виносяться на вирішення експерту. Окреслено алгоритм дій слідчого, прокурора щодо залучення експерта до проведення судової комп'ютерно-технічної експертизи. Конкретизовано методику проведення судової комп'ютерно-технічної експертизи та проаналізовано типові помилки при її проведенні, досліджено окремі аспекти оцінки уповноваженими суб'єктами висновку експерта.

Для здобувачів вищої освіти, аспірантів, ад'юнктів та викладачів вишів і факультетів юридичної спрямованості всіх форм навчання. Може бути корисним для працівників органів досудового розслідування, прокуратури, суду, експертних підрозділів.

Issue summaries theoretical information about objects judicial of computer-technical expertise, rules of engagement and storage of information. It defined tasks, subjects and a range of questions, which expert have to do, highlighted algorithm of action of the investigator, prosecutors for attracting expert to holding judicial computer-technical expertise. Methodology of realization judicial computer-technical expertise is specified. Basic mistakes which appear while computer-technical expertise is holding are analyzed. Some aspects of the evaluation by the authorized subjects of the expert opinion are investigative.

The textbook is intended for students of higher education, graduate students, associates and graduates of universities and faculties of law of all forms of education. It can be useful for employees of bodies of investigation, procurator's office, court, expert departments.

Видано в авторській редакції.

УДК 343.148

ВСТУП

Людська цивілізація швидко входить в абсолютно нову стадію свого розвитку. Тому все більш масоване проникнення цифрових інформаційних і телекомунікаційних технологій у повсякденну дійсність стала на сьогоднішній день глобальним явищем.

Невблаганне зростання кількості людей, що користуються комп'ютерними технологіями, відкрила нові можливості для злочинної діяльності. Це торкнулось і нашої країни, що підтверджується вибуховою кількістю зареєстрованих кримінальних правопорушень, вчинених з використанням комп'ютерної техніки та комп'ютерних технологій.

Вирізняє такі кримінальні правопорушення здебільшого латентний характер, вони не залишають видимої слідової картини на місці вчинення, є складними для виявлення й розкриття, що зумовлено, зокрема, як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним, у традиційному криміналістичному значенні, місцем учинення злочину – кібернетичним простором[1].

А це, у свою чергу, викликає необхідність застосування спеціальних знань у сфері інформаційних комп'ютерних технологій для розслідування кримінальних правопорушень. У зв'язку з цим зростає роль і значення комп'ютерно-технічних та інших видів експертиз електронної інформації.

[1] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 24.

У багатьох випадках призначення і проведення судової експертизи є необхідною умовою для ефективного вирішення кримінального провадження.

Судова комп'ютерно-технічна експертиза (далі – СКТЕ) – це окрема, суворо регламентована процесуальна дія, що проводиться в ході розслідування кримінальних правопорушень. Вона є основною процесуальною формою використання спеціальних знань у галузі комп'ютерних технологій, а її результати можуть являти собою найважливішу частину доказової бази у конкретному кримінальному провадженні.

Однак, щоб висновок експерта було визнано допустимим, законодавством передбачені вимоги до призначення судової експертизи, а слідчою та експертною практикою вироблено рекомендації щодо ефективного її проведення. Крім того, будь-яка експертиза повинна проводитись на підставі методики, що відповідає сучасному рівню розвитку науки і техніки. І, оскільки такий вид судової експертизи, як СКТЕ, відносно новий, при її призначенні часто виникає ряд типових помилок. Акцентування на них уваги є необхідним.

Розслідування кримінальних правопорушень, вчинених з використанням комп'ютерної техніки та комп'ютерних технологій, ускладнюється тим, що з постійним розвитком інформаційних технологій з'являються об'єкти дослідження, яких раніше просто не було, змінюються, модифікуються механізми і методи вчинення раніше відомих видів злочинів, з'являються абсолютно нові їх види. Одночасно з розвитком інформаційних технологій та інформаційних систем вченими проводяться дослідження теорії і практики протидії кіберзлочинності, розробляються алгоритмами розслідування інцидентів, аналізуються уразливості, шкідливе програмне забезпечення[2].

[2] Шелупанов А. А., Смолина А. Р. Методика проведения подготовительной стадии исследования. Доклады ТУСУРа. 2016. Т. 19. № 1. DOI: 10.21293/1818-0442-2016-19-1-31-34.

Невирішеним залишається питання спрощення пошуку окремих експертних методик проведення СКТЕ. Експертам для дачі повного, достовірного, науково обґрунтованого висновку необхідно використовувати експертні методики, які відповідають часу. Натомість, існуючі методики СКТЕ швидко застарівають і вимагають доопрацювання.

Експерти через швидке старіння методик, велику кількість об'єктів дослідження і широке коло питань даного роду експертизи значну частину часу витрачають на адаптацію і доопрацювання загальних методик під окремі завдання експертизи, пошук необхідних методів – розробку окремих методик проведення СКТЕ. Складність і тривалість розробки окремих методик СКТЕ збільшуються при накладенні експертною організацією обмежень на вибір методів проведення експертизи за ресурсами (термінами, вартістю експертного програмного забезпечення та ін.)[3].

Вищеописане підкреслює актуальність завдання удосконалення існуючих методик проведення СКТЕ.

Наслідки різного роду упущень уповноважених осіб, які здійснюють збирання такої специфічно збереженої інформації, а також непрофесійні дії фахівців у вказаній сфері, можуть мати негативну значимість, адже у такому разі завдання кримінального провадження реалізуються неповністю або частково, що в свою чергу, може спричинити прийняття необґрунтованого і незаконного підсумкового рішення у конкретному кримінальному провадженні. Необхідність зведення до мінімуму непрофесійних дій уповноважених учасників кримінального провадження, спеціалістів, експертів, використання у доказуванні допустимих доказів, диктують важливість вивчення сутності СКТЕ, завдань, які вона вирішує, а також вироблення дієвих криміналістичних рекомендацій у цьому напрямку.

[3] Шелупанов А. А., Смолина А. Р. Методика проведения подготовительной стадии исследования. Доклады ТУСУРа. 2016. Т. 19. № 1. DOI: 10.21293/1818-0442-2016-19-1-31-34.

Проблеми якості розслідування кримінальних правопорушень і судочинства залежать від рівня розробки комплексу дієвих рекомендацій щодо їх розкриття, розслідування та попередження.

Невирішеною на сьогодні залишається низка практичних проблем, пов'язаних із поводженням з електронною слідовою інформацією, призначенням та проведенням СКТЕ, використанням її результатів у кримінальному процесуальному доказуванні.

Вказані та інші чинники організаційно-тактичного та процесуального характеру обумовлюють актуальність навчального посібника, визначають їх структуру і зміст.

1 СЛІДИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЯК ОБ'ЄКТ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Ефективність розслідування кримінальних правопорушень багато в чому залежить від своєчасного виявлення слідів злочинних дій. Кримінальні правопорушення, вчинені з використанням комп'ютерної техніки, мережі Інтернет, засобів стільникового зв'язку (зокрема, ст.ст. 190, 301, 333, 366-1 КК України[4] та ін.), завдають значних матеріальних збитків, при цьому, в силу специфіки їх розслідування, злочинцям вдається тривалий час залишатися безкарними.

Під час збирання доказів при розслідуванні таких кримінальних правопорушень виникає проблема, викликана тим, що поряд з «традиційними» слідами частиною відомостей є комп'ютерна інформація, яка не залишає змін у зовнішньому матеріальному сере-

[4] Ухвала слідчого судді Приморського районного суду м. Одеси про призначення судової комп'ютерно технічної експертизи від 05.02.2019 у справі № 522/8682/18 (кримінальне провадження № 220181600000000053) URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021); Ухвала слідчого судді Вищого антикорупційного суду про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 30.09.2019 у справі № 760/24486/19 (кримінальне провадження № 42018000000002019). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021); Ухвала слідчого судді Тернопільського міськрайонного суду Тернопільської області про призначення комп'ютерно-технічної експертизи від 17.10.2018 у справі №607/21024/18 (кримінальне провадження № 12018210000000316); Ухвала слідчого судді Рівненського міського суду Рівненської області про призначення судової комп'ютерно-технічної експертизи від 16.04.2019 у справі № 569/1173/19 (кримінальне провадження № 12018180000000335). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021); Ухвала слідчого судді Самарського районного суду м. Дніпропетровська про призначення комп'ютерно-технічної експертизи від 24.05.2019 у справі № 206/2829/19 (кримінальне провадження № 12019040700000137). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

довищі, так як в більшості випадків носить інформаційний характер[5], а серед науковців і практиків інтерпретується по-різному – як електронна, цифрова, комп'ютерна, віртуальна, бінарна інформація.

В умовах суцільного проникнення інформаційно-телекомунікаційних технологій в усі сфери суспільного життя електронний доказ стає основним джерелом доказової інформації під час розгляду окремих категорій справ[6]. Електронні записи, електронна пошта, файли обробки інформації, файли із зображеннями все частіше є важливими доказами у кримінальному провадженні. Вказані цифрові сліди залишаються не тільки при учиненні кіберзлочинів. Будь-яка з обставин, що підлягають доказуванню, в наш час можуть бути представлені у цифровій формі[7]. Характерною рисою такої інформації з позиції доказування є те, що вона може виступати як безпосередній слід кримінального правопорушення, так і носій такого сліду, тобто об'єкт-слідоносій. Як і будь-який слід, комп'ютерна інформація відображає факт взаємодії матеріальних об'єктів. Однак при цьому така інформація має відмінну якість: комп'ютерна інформація легко може бути змінена або знищена, причому вказані дії можуть проводитися дистанційно.

Належність електронного відображення визначають відповідно до ст. 85 КПК України. Важливим аспектом належності електронного відображення є його здатність встановлювати факт, який входить до предмету доказування. Дослідження змісту електронного відображення та інформації в сервісних опціях операційної системи про це відображення, в загальних рисах дозволяє встановити: подію злочину (наприклад, виявляючи сайт із забороненим контентом або з контентом, оприлюднення якого обмежено за законом); особу злочинця (зокрема, вивчаючи дані його аккаунта, встановлюючи IP-адресу комп'ютера); спосіб та обставини вчинення зло-

[5] Касаткин А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дис. на соискание ученой степени канд. юрид. наук. М., 1997. С. 17-18.

[6] Павлова Ю. С. Особливості збирання та процесуального закріплення електронних доказів у цивільному судочинстві. *Науковий вісник Херсонського державного університету*. 2017. Вип. 4. Т. 1. С. 77.

[7] Олиндер Н. В. К вопросу о доказательствах, содержащих цифровую информацию. *Юридический вестник Самарского университета*. 2017. Т. 3. № 3. С. 108.

чину (наприклад, аналізуючи зміст електронного листування, результати моніторингу банківських рахунків тощо); характер і розмір шкоди, завданої злочином (які можуть полягати у порушенні функціонування певних електронних відображень, неправомірному перерахуванні електронних грошових коштів, передплаті ненаданих послуг (товарів), підробці документів, порушенні авторських прав тощо). Крім того, дослідження електронного відображення дозволяє підтвердити факти, раніше встановлені іншими доказами, а також набути аргументів для спростування фактів, що належать до інших слідчих версій[8].

Для того, щоб зазначені сліди могли перетворитись на докази, необхідно їх знайти, процесуальним шляхом виявити та зафіксувати. Основним процесуальним способом перетворення невидимої інформації та слідів кримінальних правопорушень на докази є проведення судової експертизи.

Отже, потенційна інформація, що знаходиться в слідах злочину, виявлених у електронних пристроях, телекомунікаційних системах і програмах, актуалізується і перетворюються в доказову інформацію саме шляхом використання спеціальних знань у формі судової експертизи. Адже експертиза є самостійною процесуальною формою одержання нових доказів і уточнення (перевірки) тих, що вже отримані[9].

До носіїв електронної інформації, що підлягають пошуку, відносяться: дискети, оптичні диски (CD, CD-R, CD-RW, DVD, DVD-RW), портативні накопичувачі пам'яті (флеш), процесори персональних комп'ютерів, плати пам'яті персонального комп'ютера, електронні записники, портативні комп'ютери, мобільні телефони, чіп-картки послуг мобільного зв'язку, аудіо- і відеокасети та ін.[10]

---

[8] Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства.* 2017. № 2. С. 118.

[9] Коршенко В. А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jumalul juridic national: teorie i practica*. 2017. №. 2. С. 192.

[10] Методика расследования хищений социалистического имущества. / отв. ред. В. Г. Танасевич. М., 1980. Вып. 4. С. 162–163.

НАКОПИЧУВАЧІ ІНФОРМАЦІЇ

HDD

Такі носії електронної інформації можуть містити в собі наступну доказову інформацію: а) файли з текстовими зображеннями підроблених документів або графічними зображеннями їх окремих фрагментів; б) відсканові зображення паперового документа і його окремих реквізитів; в) програмне забезпечення, за допомогою якого формувалося електронне зображення документа і його реквізитів; г) файли-сліди електронного монтажу; ґ) файли, що містять інформацію довідкового характеру щодо способів підробки документів; д) викрадені бази даних; є) незаконно скопійовані чи

генеровані коди електронного цифрового підпису; е) програмне забезпечення системи електронного документообігу; ж) шкідливі програми, що використовуються для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; з) програмне забезпечення функціонування принтера, сканера чи іншого периферійного обладнання; і) протоколи роботи в Інтернет, адреси сайтів і електронної пошти, що найбільш часто застосовуються, повідомлення електронної пошти; ї) фінансово-господарські дані («чорнова» бухгалтерія) та ін.[11].

Місцем виявлення електронних слідів можуть бути як матеріальні, так і нематеріальні об'єкти: ресурси мережі Інтернет, профіль користувача в соціальних мережах, електронні платіжні системи (PayPal, LiqPay, iPay.ua, «Qiwi», WebMoney, Perfect Money та ін.), бази даних (абонентів операторів зв'язку, криміналістичних обліків МВС та ін.), локальні мережі різних структур, «жорсткі диски» персональних комп'ютерів (ноутбуків, планшетів та ін.), карти пам'яті, засоби стільникового зв'язку і багато іншого.

В даний час одним з технічних засобів, які найбільш часто використовуються у протиправних цілях, є засоби стільникового зв'язку. Вони можуть виступати не лише носіями криміналістично значимої інформації, а й предметами, знаряддями злочинів. Наприклад, при вчиненні вимагання вже типовими є дії злочинних груп, коли по мобільному телефону висуваються вимоги про зарахування на абонентський рахунок злочинця грошових коштів за повернення викраденого транспортного засобу.

Типовими для кримінальних правопорушень, учинених з використанням засобів стільникового зв'язку будуть наступні сліди: інформаційні сліди на машинних носіях оператора зв'язку (наприклад, дані первинного номера телефону, який використовується для зв'язку та зберігається у log-файлах; дати сеансу зв'язку; інформація про час зв'язку; статичні або динамічні IP-адресні журнали реєстрації провайдера в Інтернеті і відповідні телефонні номери;

[11] Осика І. М. Поняття способу підробки документів, що використовуються при вчиненні злочинів у сфері підприємництва. *Право і Безпека*. 2005. Т. 4. № 6. С. 93.

швидкості передачі повідомлення; вихідні журналів сеансів зв'язку, що включають тип використаних протоколів, самі протоколи та ін.)[12]; сліди на самому мобільному телефоні (приміром, IMEI-код, SMS-повідомлення, відомості про надіслані повідомлення, телефонні з'єднання, абонентська книга телефону, телефонні номери, що використовуються, сліди мікрочастинок, пальців рук. Сліди, присутні на SIM-карті і наявні на мобільному телефоні, зазвичай ідентичні)[13].

Отже, електронна слідова інформація і способи її пізнання дуже тісно перекликаються з об'єктами СКТЕ[14]. Адже її родовим об'єктом є категорія предметів, що володіють загальними ознаками і відносяться до комп'ютерних засобів, серед яких виділяються програмні продукти, текстові та графічні документи, файли мультимедіа, бази даних, файли додатків, системні звіти і журнали додатків.

Враховуючи вимоги глави 4 КПК «Докази і доказування» логічно стверджувати, що електронні носії інформації з медіаконтентом можуть бути віднесені до таких джерел доказів як «речові докази» або «документи»[15].

Електронна слідова інформація, як носій інформації в складі доказів речових – предмет, що містить важливу для кримінального провадження інформацію, створену не в процесі розслідування (розкриття) кримінального правопорушення, сприйняття якої неможливе без використання електронно-обчислювальних засобів. Якщо ж виходити з кримінальної процесуальної регламентації

---

[12] Потапов С. А., Потапова И. С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. *Социально-экономические процессы и явления.* 2016. Т. 11. № 11. С. 157.

[13] Климчук М. П. Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, та особливості їх виявлення. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід.* К. : НАВС, 2020. С. 86.

[14] Усов А. И. Концептуальные основы судебной компьютерно-технической экспертизы : дис. ... д-ра юрид. наук. М., 2002. С. 97-98.

[15] Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації: Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 8.

роботи з доказами, то будь-який контент є просто комп'ютерними даними, що мають певну споживчу цінність і здатні задовольнити інформаційну потребу сторони обвинувачення (чи захисту) під час доказування обставин, що належать до предмету доказування[16].

Зважаючи на те, що електронний документ – це певний комп'ютерний код, то такий код може бути прочитаний лише за допомогою спеціальних засобів, які забезпечують тлумачення цифрового коду та його перетворення в доступну для сприйняття форму. Одночасно із цим, така особливість електронного документа як доказу зумовлює особливість його слідчого огляду як окремої процесуальної дії. Слідчий або інший учасник кримінального провадження не може дослідити електронний документ без спеціальних засобів, а тому, як правило, така процесуальна дія здійснюється за допомогою спеціального обладнання на робочому місці слідчого. При цьому огляд та дослідження фізичного носія електронного документа не є дослідженням самого електронного документа. В такому разі фізичний носій може виступати лише в якості речового доказу[17].

Виходячи з особливостей огляду та попереднього дослідження електронних документів, з якими слідчий найчастіше має справу в процесі розслідування кримінальних правопорушень, їх можна згрупувати за такими категоріями: 1) електронні документи на фізичних носіях інформації; 2) електронні документи у вигляді публікацій у мережі Інтернет; 3) електронні документи, розміщені у хмарних сервісах зберігання інформації[18].

Основною властивістю доказу, що містить електронну інформацію, є верифікованість. Інформація, яка складає зміст такого доказу, завжди повинна бути засвідчена на предмет можливості її ідентифікації і аутентифікації, тобто перевірки цілісності інфор-

---

[16] Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації: Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 8.

[17] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Серія: Право.* 2017. № 4 (58). С. 83.

[18] Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України* 2017. № 1 (88). С. 185.

мації та її незмінності на електронному носії. Вказані гарантії здебільшого знаходяться в технологічній сфері, проте забезпечення обов'язковості їх застосування в межах кримінального провадження – завдання кримінального процесу.

Від розуміння природи електронної інформації, правильного поводження з нею не лише при проведенні СКТЕ та інших видів експертиз, а й при збиранні доказів, які містять такі сліди, залежить можливість їх застосування у кримінальному провадженні.

На цьому зосередимо увагу у наступних розділах.

2 ВИЛУЧЕННЯ ТА ЗБЕРІГАННЯ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Тільки експертиза спроможна, забезпечивши отримання органами досудового розслідування унікальної розшукової інформації, створити визначене ч. 2 ст. 84 КПК України процесуальне джерело доказів – висновок експерта[19]. 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 СКТЕ[20].

Під час досудового розслідування можуть бути виявлені як матеріальні сліди (сліди пальців рук, мікрооб'єкти тощо), так і віртуальні (відвідування відповідних сайтів, архів листування користувача, управління рахунками електронних платіжних систем, геолокації та ін.), що сприяють формуванню повноцінної доказової бази і викривають не тільки його користувача, а й інших осіб, причетних до вчинення кримінального правопорушення.

Кримінальним процесуальним законодавством (зокрема, ст. 100 КПК) регламентується діяльність зі зберігання речових доказів. Електронний носій інформації, якщо він відповідає дефініції «речового доказу» (ст. 98 КПК, приміром, якщо він є матеріальним об'єктом), може бути отриманий стороною обвинувачення,

[19] Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

[20] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 28.

вилучений, взятий під контроль стороною обвинувачення за певним процесуальним порядком, оглянутий, сфотографований, описаний, скопійований, долучений до кримінального провадження, повернутий володільцю, збережений, втрачений або знищений тощо[21].

Робота з електронною слідовою інформацією – це складна процедура, яка часто вимагає спеціальних знань, а її результат буде залежати від того, наскільки швидко і якісно здійснено фіксацію, збереження та вилучення слідової інформації, що міститься в електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, інформаційно-телекомунікаційних системах або їх частинах. Такі дії необхідно виконувати з певною систематизацією, починаючи з огляду місця події, електронної техніки, джерел зовнішньої пам'яті і закінчуючи вилученням даних з електронних накопичувачів інформації, що мають відношення до кримінального провадження.

Електронні сліди, та їх носії повинні бути вилучені, зафіксовані й оформлені відповідно до вимог чинного кримінального процесуального законодавства. Надзвичайно важливим є з'ясування особливостей процедури вилучення та зберігання такої інформації з огляду на можливість її використання як об'єкта СКТЕ. Правильність вилучення об'єктів СКТЕ має велике значення для повноти і достовірності подальшого їх дослідження[22]. Тому під час досудового розслідування їх необхідно надавати незміненими, для забезпечення можливості проведення експертизи. Для пошуку електронної інформації потрібно застосовувати методи і засоби, що не модифікують першочергово вилучену інформацію на джерелі зовнішньої пам'яті.

З аналізу змісту ст. 93 КПК України випливає, що електронні відображення, як доказ, можуть бути зібрані шляхом проведення

[21] Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації. Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 8.

[22] Маринин С. А. Правовые и организационно-тактические основы выявления, документирования и раскрытия преступлений, совершаемых в сфере незаконного игорного бизнеса с использованием компьютерной техники и Интернета : монография. Н. Новгород : НА МВД России, 2015. С. 139.

слідчих (розшукових) дій та негласних слідчих (розшукових) дій, проведення інших процесуальних дій. Зокрема, електронні відображення можуть бути виявлені в ході обшуку (ст. 234 КПК), огляду (ст. 237 КПК), а також в ході тимчасового доступу до речей і документів як заходу забезпечення кримінального провадження (ст. 159 КПК). Приміром, тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення (ч. 1 ст. 159 КПК). При цьому ст. 159 КПК встановлено, що такий тимчасовий доступ можливий виключно на підставі ухвали слідчого судді. Вказану норму можна тлумачити як засіб забезпечення можливості використання копій електронних відображень як джерел доказів у кримінальному провадженні.

У ч. 2 ст. 99 КПК України зазначається, що матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, можуть бути зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність»[23]. Вказані матеріали здебільшого формуються у вигляді оперативних документів, а також електронних відображень (фотографій, фонограм та відеограм в сучасному цифровому форматі) і можуть бути використані у кримінальному провадженні як докази, бути об'єктами СКТЕ.

Слідова інформація, яка міститься у вигляді електронно-цифрових відображень, також може бути отримана в ході проведення таких НСРД, як аудіо-, відеоконтроль особи (ст. 260 КПК), зняття інформації з транспортних теле-комунікаційних мереж (ст. 263 КПК), зняття інформації з електронних інформаційних систем (ст. 264 КПК), установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК), спостереження за особою, річчю або місцем (ст. 269-1 КПК), моніторинг банківських рахунків (ст. 269 КПК), аудіо-, відеоконтроль місця (ст. 270 КПК), контроль за вчиненням злочину (ст. 271). У таких випадках електронно-цифрові

[23] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

сліди оформлюються як додаток до протоколу відповідної слідчої (розшукової) дії[24].

Частина 2 ст. 93 КПК України містить вказівку на інший спосіб збирання електронних відображень: вони можуть бути витребувані від органів державної влади, органів місцевого самоврядування, службових та фізичних осіб, підприємств, установ та організацій. Підприємствами, які відіграють ключову роль у забезпеченні обігу електронних зображень і мають технічні можливості щодо їх збереження, є провайдери Інтернет-послуг (Інтернет-провайдери) та оператори мобільного зв'язку. Недосконаліть правового регулювання їх відносини з органами розслідування призводить до численних непорозумінь, необґрунтованих вилучень слідчими мережевої комп'ютерної техніки у провайдерів, що веде до порушень прав користувачів мережі Інтернет й до визнання судом здобутих доказів недопустимими, а також породжує небажання провайдерів надавати інформацію правоохоронним органам[25].

Отже, питання кваліфікованого збирання доказів у кримінальних провадженнях, вчинюваних з використанням електронних носіїв інформації (комп'ютерних блоків, серверів, ноутбуків, мобільних засобів зв'язку, карт пам'яті та ін.), потребує належної законодавчої регламентації відповідних процедурних повноважень органів досудового розслідування.

Так, у одному із проектів Закону України «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність та підвищення ефективності боротьби з кіберзлочинністю» з-поміж іншого було запропоновано внести відповідні зміни до КПК України, які стосуються: надання можливості правоохоронним органам здійснювати термінове збереження інформації, що значно підвищить ефективність відслідковування та попередження вірусних атак; можливості у виняткових невідкладних випадках здійснювати тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, до

[24] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

[25] Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 117.

постановлення ухвали слідчого судді, суду; можливості під час проведення обшуку законним чином отримувати доступ до комп'ютерних систем, які фізично розташовані за межами місця проведення обшуку, долати системи логічного захисту, отримувати інформацію про особливості функціонування комп'ютерних систем та застосовані щодо них заходи захисту; вдосконалення процедури проведення негласних слідчих (розшукових) дій під час досудового розслідування злочинів, передбачених розділом XVI КК України.

Будь-яка інформація, яка передається за допомогою інформаційно-телекомунікаційних систем, зберігається на спеціальних технічних носіях (серверах) і в спеціальному вигляді (log-файлі). Інтернет-провайдери та інші суб'єкти, які беруть участь у процесі інформаційно-телекомунікаційної передачі даних та у фактичному володінні яких перебувають сервери, мають можливість вилучити необхідні log-файли, засвідчити їхній зміст та надати на вимогу уповноважених учасників кримінального провадження. Такий спосіб збирання доказової інформації, у т. ч. електронної, використовується під час розслідування кримінальних правопорушень шляхом проведення відповідних НСРД.

Зауважимо, що загалом власники серверів досить неактивно співпрацюють з правоохоронними органами або ігнорують запити, апелюючи щодо відсутності технічної можливості зберігання даних. Слід також наголосити, що сучасні месенджери «WhatsApp» і «Viber» містять шифрування end-to-end, що технічно унеможливлює дешифрування листування для компанії, якій належить месенджер, а вся переписка знаходиться під контролем користувачів. Виходить, що правоохоронні органи не зможуть традиційними способами одержати інформацію про листування абонентів.

Вразливість» електронного документа зумовлює необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів кримінального провадження. Зокрема, на рівні з традиційними правилами поводження із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації[26].

[26] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Серія: Право*. 2017. № 4 (58). С. 84.

В ході обшуку та огляду приміщення, місцевості електронні відображення, які містять відомості, що мають значення для кримінального провадження, можуть бути виявлені: 1) в обшукуваному (оглянутому) приміщенні, на місцевості: на автономному електронному носієві (флешка, автономний електронний накопичувач), на спеціалізованому пристрої (смартфон, цифровий фотоапарат, цифровий диктофон тощо) або на пристрої пам'яті стаціонарного комп'ютера (ноутбука); 2) в мережі Інтернет поза межами обшукуваного (оглянутого) приміщення, місцевості, а саме на віддаленому сервері, доступ до змісту якого здійснюється із комп'ютера, розташованого у зазначеному приміщенні[27].

Будь-які дії з електронними документами мають здійснюватися у визначеному законом порядку уповноваженими особами за допомогою сертифікованого службового обладнання, з використанням ліцензійного програмного забезпечення. Використання несертифікованого обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з електронного документа через апаратні та/або програмні збої та помилки.

Процес огляду електронних документів в цілому відповідає загальноприйнятому алгоритму дій, які вчиняються слідчим під час огляду звичайних документів. Такий комплекс дій повинен складатися з наступного: 1) пошук і виявлення документів; 2) візуальний огляд зовнішнього стану без зміни умов сприйняття; 3) фіксація за допомогою фотозйомки; 4) фіксація в протоколі відповідної слідчої (розшукової) дії (фіксуються всі дії посадових осіб, стан документа і виявлені сліди); 5) виявлення слідів рук (на фізичному носії електронного документа); 6) виявлення слідів зміни первісного змісту; 7) підготовка до упаковки; 8) упаковка[28].

На наше переконання, огляд предметів, у т. ч. електронних носіїв інформації (комп'ютерних блоків, серверів, ноутбуків, карт пам'яті), повинен проводитися за місцем їх виявлення, як правило,

---

[27] Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 118.

[28] Бірюков В. В. Криміналістичне документознавство. К. : Паливода А. В. 2007. С. 129.

при огляді, за участю спеціаліста. Саме слідчий складає протокол про їх виявленні, в якому фіксуються їх індивідуальні ознаки[29]. Його основними завданнями під час виявлення і вилучення документів на комп'ютерних носіях інформації є: 1) належним чином вилучити носії комп'ютерної інформації та периферійні пристрої (за наявністю) і зафіксувати це в протоколі; 2) належним чином упакувати всі елементи апаратно-програмного комплексу і носії інформації; 3) відправити їх для експертного дослідження в лабораторних умовах; 4) забезпечити цілісність інформації і запобігти її знищенню чи пошкодженню на всіх етапах роботи з нею[30].

Слід наголосити, що конкретні об'єкти пошуку залежать від виду злочину, що розслідується, способу його вчинення, а також властивостей документа і, відповідно, пошуку та вилучення. Наприклад, об'єктами пошуку при розслідуванні незаконних дій з банківськими платіжними картками будуть: а) заготовки, викрадені чи виготовлені картки; б) носії комп'ютерної інформації з даними реквізитів карток, програмним забезпеченням для генерації номерів карток, зламу баз даних, копіювання і записування номерів карток; в) обладнання для виготовлення карток або внесення до них змін (ембосери, термопринтери, ламінувальні машини та ін.); г) сканери; ґ) цифрові камери; д) матеріал для виготовлення карток (пластик, фольга, магнітна плівка); є) мобільні телефони; ж) карти або схеми населених пунктів з поміченими на них місцями розташування банкоматів; з) шматки паперу з написами, що можуть виявитися паролями і кодами доступу до електронної пошти та інших інформаційних ресурсів тощо[31].

Під час застосування такого заходу забезпечення кримінального провадження, як *тимчасовий доступ до речей та документів* (163 КПК України) електронні носії інформації можуть бути оглянуті, а їх вміст скопійовано. Також слідчий суддя, суд в ухвалі про

---

[29] Виницкий Л. В., Мельник С. Л. Экспертная инициатива в уголовном судопроизводстве. М. : Экзамен, 2009. С. 81.

[30] Осика І. М. Поняття способу підробки документів, що використовуються при вчиненні злочинів у сфері підприємництва. *Право і Безпека*. 2005. Т. 4. № 6. С. 94.

[31] Там само.

надання тимчасового доступу до речей і документів може дати розпорядження про надання можливості вилучення речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що без такого вилучення існує реальна загроза зміни або знищення речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів (п. 7 ст. 163 КПК України).

За загальним правилом, якщо електронно-цифрова інформація міститься на серверах чи жорстких дисках підприємств, установ, організацій, слід здійснити побітову копію носія інформації, адже вилучення майна вказаних юридичних осіб може призвести до негативних наслідків. Ідентична копія електронної інформації, яка знаходиться на технічному носії, має бути відтворена за допомогою спеціального обладнання, після чого самі фізичні носії повертаються власникам. В подальшому скопійована слідова інформація може бути надана на дослідження у разі призначення у кримінальному провадженні СКТЕ. Доцільно також зазначити, що аналогічного алгоритму дій необхідно дотримуватись у разі виникнення необхідності у проведенні СКТЕ.

З огляду на особливості фізичної форми інформації, що міститься на електронних носіях, процесуальні норми, що регламентують особливості формування доказів на основі такої інформації, повинні гарантувати її збереження під час усього кримінального провадження, в тому числі і у випадках, коли електронний носій з певних причин залишається у законних власників.

Варто також акцентувати увагу на тому, що особливості огляду електронної слідової інформації залежно від фізичних особливостей носія, який її містить. Зважаючи на специфіку кожного з таких носіїв, особливості виявлення та збереження інформації, яку вони містять, а також на предмет дослідження, обмежимось їх перерахуванням:

– електронні документи, розміщені на фізичному носії інформації (зовнішні фізичні носії пам’яті електронно-обчислювальної машини (жорсткий диск – HDD, SDD; дискові носії – CD, DVD, Blue-Ray-диски, дискети; USB-диски); оперативний запам’ятовуючий пристрій (далі – ОЗП) ЕОМ; ОЗП периферійних пристроїв (наприклад, принтер, у пам’яті якого знаходяться

документи у «черзі друку»); ОЗП пристроїв зв'язку тощо[32]; флеш-карти пам'яті (SD, micro SD тощо)[33];

– електронні документи, розташовані у пам'яті засобів стільникового зв'язку;

– публікації, які містяться у мережі Інтернет;

– електронні документи, розміщені у «хмарних» сервісах зберігання інформації.

До початку фізичного огляду комп'ютерної техніки слідчий повинен встановити технічні пристрої та технології, що задіяні на даному об'єкті для захисту інформації. Це встановлюється шляхом як опитування осіб, котрі відповідають за безпеку об'єкта, так і вивчення технічної документації по захисту інформації на об'єкті. При цьому з'ясовуються такі обставини:

1) чи заблоковане приміщення, в якому перебуває комп'ютер, електронною системою допуску або охоронною сигналізацією, і які технічні засоби використовуються для цього;

2) чи встановлені в комп'ютері спеціальні засоби для знищення інформації у разі спроби несанкціонованого доступу до неї; з'ясувати місце перебування організації, що встановила цю систему;

3) чи необхідні пароль (додатковий пристрій – електронний ключ) для доступу до інформації, що знаходиться в комп'ютері, або окремих її частин, правила його використання;

4) чи з'єднані (включені) комп'ютери в локальну мережу установи, організації, підприємства (фірми), об'єднання, яка схема локальної мережі, основні правила її безпечного використання[34]?

Якщо комп'ютер підключений до мережі Інтернет, то необхідно вилучити договори у керівника підприємства (фірми), де буде проводитись огляд, негайно зв'язатися з мережним адміністрато-

---

[32] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М. : ООО «Юрлитинформ», 2001. С. 149–150.

[33] Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України* 2017. № 1 (88). С. 183.

[34] Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).

ром – провайдером вузла, до якого підключена дана установа (підприємство, організація), і організувати за його допомогою вилучення і збереження електронної інформації, що належить даному підприємству або надійшла на його адресу. В такому разі оперативним шляхом доречно встановити, чи зберігає власник усі свої дані у зовнішньому сховищі, і якщо це так, то інформацію на локальних машинах можна не виявити і необхідно з'ясувати доступ до зовнішнього накопичувана;

5) у осіб, відповідальних за резервне копіювання і збереження протоколів, з'ясовується місцезнаходження відповідних документів і копій на магнітних носіях та вживаються заходи з їх вилучення та збереження[35];

При проведенні фізичного огляду необхідно: наказати співробітникам фірми (підприємства) відійти від комп'ютерних засобів і розмістити їх у приміщенні так, щоб виключалась можливість використання будь-яких засобів зв'язку. У процесі огляду не приймати допомоги від співробітників фірми (підприємства); вилучити у персоналу пейджери, електронні записні книжки, ноутбуки, індивідуальні пристрої відключення сигналізації автомобіля тощо; зафіксувати інформацію на екранах працюючих комп'ютерів шляхом фотографування (детальна зйомка); виключити живлення міні-АТС і опечатати її (якщо така є); скласти схему підключення зовнішніх кабелів до комп'ютерних пристроїв і позначити кабелі для правильного відновлення з'єднання в майбутньому; ізолювати комп'ютери від усякого зв'язку ззовні: модемної, локальної комп'ютерної мережі, радіозв'язку; найбільш ефективним способом відключити всі комп'ютерні засоби від джерел живлення (у тому числі і від джерел безперебійного живлення)[36].

Фахівець оперативно виконує дії відповідно до плану, розробленого спільно зі слідчим. Зовнішнім оглядом встановлюються специфічні обставини, що стосуються комп'ютерних засобів, дані про які заносяться до протоколу огляду комп'ютерного засобу:

---

[35] Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).

[36] Там само.

наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела живлення, акустичних систем тощо, периферійних і мультимедійних пристроїв.

За розташуванням частин пристроїв на передній панелі системного блоку фахівець визначає їх види (пристрої збереження інформації, дисководи), а також види пристроїв зчитування кредитних карт, смарт- чи чіп-карт тощо. Особливої уваги потребують наявні не відомі йому пристрої. За розташуванням розйомів на задній панелі системного блоку визначаються наявність і види вбудованих пристроїв, мережної плати, модему (чи був він підключений до телефонної чи іншої лінії зв'язку), наявність послідовних і паралельних портів, чи були вони підключені до зовнішніх ліній зв'язку[37].

У протоколі необхідно навести схему підключення кабелів до комп'ютерної системи. Кабелі, що відключаються, підлягають маркуванню з метою відновлення з'єднання при проведенні експертизи комп'ютерної техніки і програмних продуктів. Системний блок комп'ютера, принтер, виявлені дискети, магнітні стрічки й інші носії комп'ютерної інформації (наприклад роздруківки) упаковують і вилучають. Упаковка об'єктів має унеможливлювати як доступ до об'єктів, так і їх пошкодження у процесі збереження чи транспортування[38].

Погоджені дії слідчого і фахівця при огляді і вилученні речових доказів з місця події дозволять уникнути незворотних втрат інформації, що міститься на машинних носіях.

Вилучення електронних носіїв інформації з різних джерел зовнішньої пам'яті під час проведення слідчих (розшукових) дій не потребує обов'язкового залучення спеціаліста до їх огляду та вилучення. Не вимагає цього й КПК України. Однак варто зазначити, що подекуди, через особливості самих об'єктів, які мають значення у кримінальному провадженні, віднайти їх може тільки фахівець у певній галузі. У досліджуваних випадках найкраще використову-

[37] Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).

[38] Там само.

вати допомогу фахівця з комп'ютерної техніки та програмного забезпечення.

На нашу думку, до таких випадків необхідно віднести: копіювання інформації з електронних носіїв інформації на інший електронний носій; встановлення наявності зв'язку між засобами комп'ютерної техніки та каналами електрозв'язку за схемами: «комп'ютер-комп'ютер», «комп'ютер-сервер» та ін.; необхідність відключення локальної мережі від технічних пристроїв; необхідність піддати обшуку сам сервер, так як саме він зберігає в своїй пам'яті найбільшу частину комп'ютерної інформації та керує робочими станціями локальної мережі.

Участь спеціаліста при вилученні електронних носіїв інформації та у слідчих (розшукових) діях, в результаті яких вилучається така інформація, дозволить усунути сумніви в достовірності отриманих доказів і є гарантією захисту прав учасників процесу під час виконання зазначених дій. Справедливим є твердження про те, що не існує такого поняття, як універсальний комп'ютерний експерт. В якості комп'ютерного експерта можливо залучати осіб з наступними спеціальностями: а) комп'ютерні науки та інформаційні технології; б) інженер з технічного захисту інформації; в) комп'ютерна інженерія; г) системна інженерія; д) програмна інженерія; е) мережеві технології та системне адміністрування; ж) аналітика комп'ютерних систем. Тому, збираючись на місце події, важливо з'ясувати, з якою технікою і з якою операційною системою доведеться мати справу[39].

Природньо, що зростання рівня й інтенсивності використання спеціальних знань призводить і до підвищення вимог до кваліфікації спеціаліста. Якісне і повноцінне проведення слідчих (розшукових) дій з використанням комп'ютерних знань спеціаліста сприяє встановленню специфіки вчиненого кримінального правопорушення, а також своєчасному його виявленню, розкриттю і розслідуванню.

Отже, при проведенні слідчого огляду, обшуку, інших процесуальних дій, пов'язаних з вилученням різних електронних носіїв

[39] Експертизи у судочинстві України: наук.-практ. посібник / заг. ред. В. Г. Гончаренка, І. В. Гори. К. : Юрінком Інтер, 2014. С. 64.

інформації, слідчі та інші співробітники повинні ретельно планувати організаційно-тактичні дії з урахуванням знань про специфіку роботи з електронними носіями інформації. Насамперед, необхідно встановити, – це тип операційної системи. Не всі комп'ютерні системи однаково розповсюджені, і тут теж можуть виникнути певні проблеми. Спеціаліст з операційної системи Windows може не володіти необхідними знаннями для управління машиною з іншою операційною системою, наприклад, Unix, Linux, OS/2, MacOS і інші. Але, незважаючи на певні труднощі, фахівець має визначитись, може він особисто працювати з даною операційною системою чи слід залучати іншого фахівця в цій галузі. В останньому випадку дії з обладнанням залучених осіб мають ретельно фіксуватися[40].

З огляду на важливість для проведення СКТЕ об'єктів, наданих на дослідження, доцільним вважаємо окрему увагу зосередити на технічних особливостях вилучення та збереження електронної слідової інформації, виявленої під час проведення слідчих (розшукових) дій.

Варто виокремити два способи отримання електронної слідової інформації: 1) вилучення усіх виявлених засобів комп'ютерної та іншої техніки з подальшим вивченням інформації, яка на ній міститься; 2) дослідження усієї інформації на електронних носіях безпосередньо під час проведення огляду чи обшуку (за наявності достатніх підстав). Останній варіант передбачає подальше копіювання інформації, яка представляє інтерес для кримінального провадження і (або) вилучення магнітних носіїв з такою інформацією.

Дії з електронною слідовою інформацією мають певний алгоритм. Так, наприклад, при вилученні електронної техніки потрібно виявити всі можливі джерела зовнішньої пам'яті як всередині електронного пристрою, так і віддалено підключені шляхом локальних обчислювальних мереж, використовуючи можливості бездротових технологій передачі інформації. Відомі випадки, коли при вилученні системного блоку співробітники оперативних підрозділів не враховували, що жорсткий диск може бути підключений віддалено з передачею даних через радіоканал, і направляли на

[40] Експертизи у судочинстві України: наук.-практ. посібник / заг. ред. В. Г. Гончаренка, І. В. Гори. К. : Юрінком Інтер, 2014. С. 66.

експертизу даний блок без накопичувача на жорсткому магнітному диску, який був підключений до комп'ютера за допомогою радіозв'язку і знаходився у припаркованому поблизу будівлі автомобілі[41].

Вилучення всіх засобів комп'ютерної техніки прискорює сам процес розслідування, дає можливість спрямувати всі сили на пошук інших матеріальних слідів, що мають відношення до кримінального правопорушення (документи, технічні засоби та ін.); знижує психологічне навантаження на громадян; не вимагає залучення висококваліфікованого фахівця у сфері комп'ютерних технологій до безпосереднього участі в обшуку, так як грамотне вилучення засобів комп'ютерної техніки цілком доступне й фахівцеві «середньої руки».

До безсумнівних переваг такого підходу можна віднести і можливість в подальшому більш детально, залучаючи необхідних фахівців, вивчити усю інформацію, наявну в пам'яті комп'ютера. Це практично виключає можливість упустити навіть професійно приховану інформацію. Однак, з іншого боку, в ряді випадків існують суто технічні труднощі вилучення усіх засобів комп'ютерної техніки (об'єднання у різноманітні мережі, можливість втрати інформації при відключенні тощо) або таке вилучення просто недоцільне. Також слід пам'ятати, що вихід з ладу комп'ютерних банківських систем і ряду підприємств може призвести до повної дезорганізації їх роботи і значних матеріальних збитків, що загрожує претензіями з їх боку. У зв'язку з цим іноді рекомендується застосовувати інший спосіб: вилучення інформації із засобів комп'ютерної техніки безпосередньо в ході проведення огляду чи обшуку. І тут не обійтись без електронного копіювання інформації з використанням переносного комп'ютера, флеш-накопичувача тощо.

При проведенні слідчої (розшукової) дії, пов'язаної з вилученням електронних носіїв, слідчий повинен чітко знати особливості вилучення і упаковки даних об'єктів з метою виключити будь-

[41] Кувычков С. И. О современных проблемах проведения судебно-компьютерных экспертиз в ходе предварительного расследования. *Вестник Нижегородской академии МВД России*. 2016. № 2 (34). С. 296.

які маніпуляції з об'єктами під час їх транспортування. Тому на підготовчому етапі слідчого огляду, обшуку слідчому необхідно враховувати, який електронний носій буде об'єктом слідчої (розшукової) дії. Адже в процесі огляду процесуальна особа може зіткнутися як з персональним комп'ютером, системними блоками, засобами стільникового зв'язку, відеореєстраторами та іншою комп'ютерною технікою, так і іншими об'єктами, наприклад, жорсткими дисками, замаскованими під інші об'єкти, нестандартною формою флеш-накопичувачів з USB-входом у вигляді іграшок, прикрас, брелока для ключів.

Виявлення, фіксація, вилучення, збереження і дослідження будь-якого об'єкта має на меті ретельне проведення кожного з етапів. Як свідчить практика, непоодинокими є випадки порушення або неякісного виконання одного з названих етапів роботи з об'єктами. Зазвичай, це вилучення і збереження слідової інформації, повноту і якість якої забезпечує упаковка виявлених об'єктів. Від того, наскільки правильно і грамотно буде упакований виявлений носій інформації, залежить результат експертного дослідження[42].

При упаковці в картонну коробку ділянки, що мають доступ до внутрішнього вмісту, оклеюються. У разі відсутності пакетів або коробок дозволяється обклеювати системні блоки аркушами паперу так, щоб виключити доступ до кнопок включення / вимикання / перезавантаження, роз'ємів для підключення живлення і гвинтів, які кріплять бокові і верхні стінки до корпусу. На практиці ж інспектори-криміналісти стикаються з недотриманням правил упаковки системних блоків: як правило, це аркуш паперу з написом, приклеєний за допомогою прозорої липкої стрічки «скотч» до верхньої кришки. Така упаковка не відповідає вимогам нормативно-правових актів і забезпечує вільний доступ до всіх роз'ємів і кнопок включення/вимикання/перезавантаження.

Головна вимога до упаковки електронних носіїв – виключити доступ до інформації на носії і можливість внесення змін у вміст пам'яті носія вже після його вилучення. Так, при виявленні мобіль-

[42] Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий. *Вестник Казанского юридического института МВД России*. 2018. Т. 9. № 2. С. 276.

ного телефону фахівці рекомендують вилучати об'єкт разом з мережевим кабелем телефону, упаковувати в картонні коробки, застосовувати відповідні програмно-апаратні комплекси, щоб виключити будь-які маніпуляції з телефоном, а саме, умисне або ненавмисне включення/вимикання телефона, зміну інформації в пам'яті мобільних пристроїв[43].

Після ретельного обстеження комп'ютерного обладнання робиться опис програмної та апаратної складової комп'ютерів. Під час опису комп'ютерів можливо використовувати наступні програмні продукти: AIDA64, Everest. Також можливо використовувати вбудовану утиліту «відомості про систему», для чого в вікні програми «виконати» (запуск виконується комбінацією клавіш win + r) набираємо msinfo32 та тиснемо на кнопці Enter. Відомості про апаратні та програмні компоненти комп'ютерів заносяться до протоколу огляду комп'ютерної техніки та завіряться двома свідками. Документ з описом комп'ютера бажано зберігати разом з вилученою технікою. Корпус повинен бути опечатаний. Печатка завірена особою-ініціатором проведення виїмки та підписами свідків. Опечатування проводити у місцях стику основного корпусу комп'ютера та бокових знімаючих кришках. Опечатувати необхідно також передню частину комп'ютера[44].

Магнітні носії, на які передбачається копіювати інформацію, мають бути підготовлені (необхідно впевнитись, що на них нема ніякої інформації). Носії потрібно зберігати у спеціальних упаковках або загортати у чистий папір (не слід використовувати звичайні поліетиленові пакети). Слід пам'ятати, що інформація може бути зіпсована вологістю, температурним впливом або електростатичними (магнітними) полями[45].

---

[43] Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий. *Вестник Казанского юридического института МВД России*. 2018. Т. 9. № 2. С. 277.

[44] Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : методичні рекомендації: Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 24.

[45] Там само. С. 25.

Під час транспортування комп'ютерного обладнання слід поводитися з ним обережно, оскільки інформація на жорсткому диску може бути пошкоджена під час транспортування. Для транспортування великих комп'ютерних систем слід підготувати транспорт та спеціальні упаковки. При вилученні й перевезенні комп'ютерів не можна ставити їх один на один, розміщувати на них будь-які інші предмети. Крім того, в ході процесуальних дій, об'єктами яких є комп'ютерна техніка, системні блоки персональних комп'ютерів, слідчий повинен уточнити у законного власника, чи є парольний захист на носії, якщо так, то вказати його в протоколі огляду (обшуку) і вкласти цю інформацію в упаковку об'єкта, так як відсутність цієї інформації збільшить тривалість експертного дослідження. Має специфічні особливості і упаковка даних об'єктів. Найнадійнішою є упаковка об'єктів у пластиковий пакет (мішок) або коробку. При цьому горловина пакета прошивається ниткою, вузол нитки оклеюється биркою з пояснювальним надписом[46].

Відеореєстратори як електронні носії інформації доцільно вилучати цілком, без вилучення накопичувача на жорстких магнітних дисках через особливості запису відеопотоку. Якщо доводиться вилучати накопичувач інформації без відеореєстратора, то в цьому випадку треба обов'язково відобразити в пояснювальних написах на упаковці повне найменування відеореєстратора з маркувальними позначеннями.

При вилученні стаціонарних відеореєстраторів не слід вилучати з них накопичувач інформації, так як відеореєстратори використовують для запису і зберігання відеоінформації свою файлову систему. Крім того, накопичувач, вилучений з відеореєстратора і потім встановлений назад, може бути переініціалізований відеореєстратором і дані можуть бути втрачені. Необхідно також вилучати блоки живлення відеореєстраторів.

При вилученні *сервера* необхідно вилучати повністю системний блок, так як накопичувачі в сервері можуть бути об'єднані в RAID-масиві різної конфігурації. Налаштування же RAID-масиву

[46] Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий. *Вестник Казанского юридического института МВД России*. 2018. Т. 9. № 2. С. 277.

в більшості випадків зберігаються в пам'яті RAID-контролера, який знаходиться всередині системного блоку. Витяг одних накопичувачів призведе до того, що експертові не буде відома конфігурація RAID-масиву і дослідження інформації буде неможливим або вкрай ускладненим[47].

При вилученні *засобу стільникового зв'язку* слід звертати увагу на його стан. Якщо телефон включений, то найкращим способом його ізоляції буде активування в ньому «автономного режиму» або режиму «в літаку». Вимкнення телефону може активувати засоби захисту (наприклад, ПІН-код для сім-карти і / або коди безпеки), які потім будуть потрібні для отримання доступу до пристрою, тим самим унеможливить проведення експертизи. У разі наявності активованих засобів захисту (наприклад, «графічний ключ») варто відразу ж поцікавитися у власника телефону алгоритмом розблокування. Слід звертати увагу на дату і час, зазначені на екрані телефону, якщо він включений, і порівнювати їх з поточним часом і датою на момент огляду, фіксуючи невідповідності.

При вилученні *даних мобільних додатків* у якості джерела електронних доказів необхідно використовувати спеціалізований софт. Прикладами таких прикладних програм є EnCase, Smartphone Examiner, MOBILedit, Forensic, Mobile Phone Examiner Plus та ін. Ці інструменти розроблені для співробітників правоохоронних органів і фахівців інформаційної безпеки з метою збирання доказів з мобільних пристроїв, вони дозволяють фізично отримувати логічні дані з пристроїв, отримати образ операційної системи, що включає файлову систему. Після проведення аналізу мобільних пристроїв можливе перенесення зібраної інформації у спеціалізовану програму FTK (Forensic Toolkit) для подальшого вивчення, наприклад, з метою відновлення видалених файлів. Також ця інтеграція дозволяє зробити кореляцію доказів, зібраних на мобільних пристроях, з доказами, зібраними на комп'ютерах[48].

---

[47] Перякина М. П., Унжакова С. В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. *Сибирский юридический вестник*. 2019. № 3-861. С. 83.

[48] Сергеев М. С. Критерии доказывания электронных преступлений при применении мобильных приложений. Особенности их изъятия. *Актуальные проблемы экономики и права*. 2016. Т. 10. № 2. С. 268.

Процедура вилучення доказів з мобільних пристроїв відрізняється від вилучення інформації з персональних комп'ютерів з огляду на те, що мобільні електронні пристрої, в порівнянні з персональними комп'ютерами, мають більш вузькі завдання, відмінну архітектуру процесора, операційну систему та ін. У зв'язку з цим методи і особливості проведення процесуальних дій повинні бути індивідуальними, залежно від технічних характеристик джерела доказів[49].

Британською асоціацією керівників поліцейських служб (ACPO) була розроблена інструкція з вилучення доказів із мобільних пристроїв[50]. Згідно із запропонованими рекомендаціями, при проведенні процесуальних дій необхідно ізолювати пристрій від мобільного з'єднання шляхом виключення пристрою або завдяки спеціальним пристроям, що глушать зв'язок, усі необхідні процедури повинні проводитися у спеціально обладнаному приміщенні. Пристрій повинен бути повністю зарядженим з метою запобігання втраті інформації при проведенні процесуальних дій. Слід враховувати особливість оперативної (RAM) пам'яті пристрою, для збереження даних на якій необхідна наявність безперебійного живлення на відміну від постійної (ROM) пам'яті. З метою збереження важливої інформації спеціаліст повинен суворо дотримуватися правил, не допускати оновлення програм, так як це може спричинити знищення даних. Разом з даними додатків, що знаходяться на мобільному пристрої, необхідно також запросити відомості, що зберігаються на серверах розробників додатків і дані Інтернет-провайдера[51].

Сучасні смартфони, особливо iPhone, часто синхронізують з комп'ютером або ноутбуком. Відповідно, доцільним буде вилучен-

---

[49] Sammons J., Brunty J. Mobile device forensics: threats, challenges and future trends. *Digital Forensics: Threatscape and Best Practices. Syngress*. 2015. P. 69.

[50] Good Practice and Advice Guide for Managers of e-Crime Investigation. URL: http://www.acpo.police.uk/documents/ crime/2011/201103CRIECI14.pdf (дата звернення: 12.03.2021).

[51] Сергеев М. С. Критерии доказывания электронных преступлений при применении мобильных приложений. Особенности их изъятия. *Актуальные проблемы экономики и права*. 2016. Т. 10. № 2. С. 268. DOI: http://dx.doi.org/10.21202/1993-047X.10.2016.2.264-272

ня у власника смартфона комп'ютера або ноутбука. Альтернативою вилучення комп'ютера або ноутбука може бути перевірка на наявність програмного забезпечення Apple на зазначеному пристрої. Не слід витягати карти пам'яті, сім-карти й інше апаратне забезпечення, яке міститься в телефоні. Упаковка вилученого комп'ютерного засобу або накопичувача інформації повинна забезпечувати, насамперед, інформаційну цілісність, тобто виключати можливість підключення кабелів електроживлення або периферійних пристроїв. Найкращим варіантом упаковки є поміщення вилученого комп'ютерного засобу цілком у полімерний пакет (мішок).

При описі комп'ютерних засобів, що вилучаються і оглядаються, слід вказувати інформацію в тому обсязі, який дозволить однозначно ідентифікувати вилучений засіб. У більшості випадків достатньо вказати марку, модель, індивідуальний заводський номер пристрою. У разі, якщо з певних причин згадана інформація недоступна, слід вказувати інші індивідуальні ознаки: розмір, колір, форму тощо. Бажано здійснювати фіксацію не тільки процесуальним способом, відображаючи вилучення електронних носіїв у протоколі слідчої (розшукової) дії, але й криміналістичним, фотографуючи об'єкт вилучення[52].

Отже, електронні документи є важливим джерелом доказової та орієнтуючої інформації у кримінальному провадженні. Залежно від того, розміщені такі документи на фізичних носіях інформації, у відкритому доступі в мережі Інтернет, чи у хмарних сервісах зберігання інформації, має бути дотримана специфічна процедура їх слідчого огляду та попереднього дослідження з метою подальшого використання у кримінальному провадженні, зокрема, при проведенні СКТЕ.

Залучення до участі в проведенні слідчого огляду, обшуку, інших процесуальних дій, спеціаліста у галузі комп'ютерної техніки, який володіє знаннями про способи виявлення та вилучення відповідної електронно-цифрової слідової інформації, спрямоване на вирішення завдань контекстного пошуку інформації, виявлення

[52] Перякина М. П., Унжакова С. В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. *Сибирский юридический вестник*. 2019. № 3-861. С. 84.

програм електронного документообігу, перегляду історії відвідувань Інтернет-оглядачів (браузерів) тощо. У своїй діяльності спеціаліст може використовувати такі інструменти, як аналіз файлів системного реєстру, службових файлів прикладних програм, системи віртуалізації і комплекси відновлення й аналізу віддалених даних, застосування програмно-апаратних комплексів тощо.

Застосування даного інструментарію, хоча й вимагає значно більших витрат часу, воно безумовно, позитивним чином відображається на результативності виявлення криміналістично значимої інформації, яка може бути надзвичайно важливою під час проведення СКТЕ.

3 ЗАВДАННЯ, ПРЕДМЕТ ТА ОБ'ЄКТ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ ТА ПИТАННЯ, ЯКІ ВИНОСЯТЬСЯ НА ВИРІШЕННЯ ЕКСПЕРТА

Завдання СКТЕ, як засобу доказування, полягає в отриманні юридично значимої інформації, що допомагає встановити факт і/або обставини злочинної події.

СКТЕ здатна забезпечити вирішення таких *основних експертних завдань*:

– 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 з 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[53].

У відповідності із завданнями і специфікою об'єктів дослідження на теперішній час в рамках такого роду експертиз, як СКТЕ, можливо виділити самостійні експертні види:

• *Експертиза комп'ютерної техніки* (*апаратно-комп'ютерна)* шляхом проведення діагностичних досліджень встановлює факти й обставини, що мають значення у кримінальному провадженні і пов'язані із закономірностями функціонування та експлуатації технічних засобів комп'ютерної системи (електричних, електронних та механічних схем, блоків, приладів та пристроїв, що містять матеріальну частину комп'ютерної системи). Основними завданнями цього виду експертизи є встановлення комплектації, технічного стану та функціональних можливостей комп'ютерної системи.

• *Експертиза програмних продуктів* (*програмно-комп'ютерна*) встановлює факти й обставини, пов'язані із закономірностями розробки та використання програмних продуктів комп'ютерної системи. Завданням цього виду експертизи є визначення функціонального призначення, технічних параметрів, вимог, алгоритму, структури, стану та особливостей програмного забезпечення.

• *Інформаційно-комп'ютерна експертиза* встановлює факти й обставини, пов'язані із закономірностями створення, обробки та збереження інформації на комп'ютерних та магнітних носіях. Її задачею є пошук, виявлення, відтворення і технічний аналіз інформації, створеної користувачем чи програмами в комп'ютерній системі[54].

---

[53] Інструкція про призначення та проведення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98. (дата звернення: 03.02.2021); Сабадаш Р. В. Судова комп'ютерно-технічна експертиза: правові підстави й особливості призначення. *Науковий вісник Чернівецького університету*. 2013. Вип. 660. С. 136; Поляков В. В. Судебная компьютерно-техническая экспертиза средств мобильной радиосвязи. *Право*. С. 142.

[54] Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1 (9). С. 141.

Комп'ютерно-мережева експертиза на відміну від попередніх ґрунтується насамперед на функціональному призначенні комп'ютерних засобів, які реалізують певну мережеву інформаційну технологію. Це дослідження призначення мережевого обладнання та збір цифрових слідів у комп'ютерній мережі. Судова комп'ютерно-мережева експертиза, виділена в окремий вид у зв'язку з тим, що лише використання спеціальних знань у сфері мережевих технологій дозволяє зібрати воєдино отримані об'єкти, відомості про них і ефективно вирішити поставлені експертні завдання. Завдання судової комп'ютерно-мережевої експертизи включають практично всі основні завдання розглянутих видів СКТЕ, тобто рішення апаратних, програмних і інформаційних аспектів встановлення фактів і обставин у кримінальному провадженні. Її об'єкти інтегровані з об'єктів описаних видів експертиз (апаратні, програмні та інформаційні), але лише з тією різницею, що вони усі функціонують в певній мережевої технології. Предметом експертизи є інформація про топологію мережі Інтернет та дані, які зберігаються на комп'ютерних та магнітних носіях та мережевому обладнанні.

Як зазначає І. І. Шапошнікова, різниця між комп'ютерно-технічною та телекомунікаційною експертизами полягає в об'єкті дослідження. Якщо, наприклад, злочин полягає у розповсюдженні вірусу (ст. 361-1 КК України) чи інформації, що міститься на комп'ютері, але має обмежений доступ (ст. 361-2 КК України), то призначати слід саме експертизу комп'ютерної техніки та програмної продукції. Проте, якщо об'єктивною стороною злочину є зчитування інформації з мереж мобільного чи супутникового зв'язку, зміна таких даних (ст.ст. 361, 363, 363-1 КК України), то призначатиметься експертиза телекомунікаційних систем та засобів[55].

Питання, які виносяться на вирішення СКТЕ, відповідно до її виду можливо розділити на дві групи.

Діагностичні:

– комп'ютер якої моделі наданий на дослідження;

[55] Шапошнікова І. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність. URL: https://ov-partners.com/osnovni-aspekty-vyboru-typu-i-provedennya-ekspertyzy-u-spravah-pro-kiberzlochynnist/?lang=ru

– які технічні характеристики його системного блоку і периферійних приладів;

– які технічні характеристики даної обчислювальної мережі;

– де і коли виготовлений і зібраний даний комп'ютер і його комплектуючі складання комп'ютера здійснювалось в заводських або кустарних умовах;

– чи співпадає внутрішня будова комп'ютера і периферія запропонованій технічній документації;

– чи не внесені в конструкцію комп'ютера зміни (наприклад, установка додаткових вбудованих приладів: вінчестерів, приладів для розширення оперативної пам'яті, зчитування оптичних дисків, інші зміни конфігурації);

– чи справний комп'ютер і його комплектуючі, який їх знос;

– які причини несправності комп'ютера і периферійних приладів;

– чи містять фізичні дефекти носії інформації;

– чи проводилась адаптація комп'ютера для роботи з специфічним користувачем (лівша, людина з вадами зору та інші);

– які технічні характеристики інших електронних засобів прийому, накопичення і видачі інформації (електронна записна книжка, телефонний сервер);

– чи справні ці засоби; які причини поломки;

– чи можливе відновлення стертих файлів, дефектних магнітних носіїв інформації; який зміст відновлених файлів;

– який механізм втрати інформації із локальних обчислювальних мереж і розподілених баз даних;

– чи маються збої у функціонуванні комп'ютера, роботі окремих програм; які причини цих збоїв; чи не викликані вони впливом вірусу (якого);

– чи поширюється негативний вплив вірусу на більшість програм, чи він діє тільки на визначені програми;

– чи можливо відновити в повному обсязі функціонування даної програми (текстового файлу), пошкодженої вірусом;

– який зміст інформації зберігається в електронній записній книжці та інше;

– чи зберігається в книжці прихована інформація і який її зміст;

– коли проводилось останнє корегування даного файлу або інсталяція даного програмного продукту;

– який був рівень професійної підготовки в галузі програмування і роботи з комп'ютерною технікою особи, яка виконувала дані дії.

Ідентифікаційні:

– чи мають комплектуючі комп'ютера (плати, магнітні носії, дисководи та ін.) єдине джерело походження;

– чи не написана дана комп'ютерна програма певною особою (вирішується комплексно при проведенні комп'ютерно-технічної і авторознавчої експертиз)[56].

Розроблення універсального переліку питань, які можуть бути поставлені перед СКТЕ при розслідуванні окремих злочинів навряд чи можливе. Проте, вважаємо доцільним навести орієнтовний перелік таких питань:

– Чи належить досліджуваний пристрій до апаратних комп'ютерних засобів?

– До якого типу (марки, моделі) належить апаратний (комп'ютерний) засіб?

– Чи в робочому стані системний блок, якщо ні, то які несправності він має?

– Чи міститься на даному носії інформація стосовно… (зазначити, яка інформація цікавить) і у якому вигляді?

– Чи містить носій досліджуваного комп'ютера інформацію про певні дії користувача (зазначити, які саме)?

– З'ясувати зміст журналу дзвінків, телефонної книги, СМС-повідомлень наданого на дослідження засобу стільникового зв'язку.

– Чи міститься в пам'яті наданих на дослідження стільникових телефонів інформація про список контактів, журнал дзвінків, текстові та мультимедійні повідомлення, веб-історії, повідомлення в Інтернеті, а також текстові, графічні, відеофайли користувача?

[56] Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації. Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 46–48.

За наявності цієї інформації скопіювати її на окремий носій інформації.

– Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

– Чи могла бути створена зазначена інформація на цьому комп'ютері, чи вона перенесена з іншого носія цифрової інформації?

– У який спосіб інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)?

– Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

– Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст, а також за можливості необхідно надати хеш-суму конкретного файлу в форматі MD5, що дозволить спів ставити файли, надані на дослідження)?

– Чи містить накопичувач інформації досліджуваного об'єкта програмне забезпечення (зазначити назву або функціональне призначення, а також вид – встановлене чи невстановлене)? (Щодо грального бізнесу – iConnect, Gaminator, iGaming Casino, iChampion, G-slot, Superomatic, Megasuperomatic).

– Чи міститься на наданих на дослідження об'єктах програмне забезпечення, призначене для віддаленого керування комп'ютером (TeamViewer, Ammyy Admin, Radmin, UltraVNC тощо)? Якщо так, чи містяться на наданих на дослідження об'єктах log-файли використання виявлених програм?

– Чи наявні на наданих на дослідження об'єктах програми, призначені для спілкування в Інтернеті (Skype, WhatsApp, Viber, Telegram тощо)? Якщо так, чи містять вони інформацію про історію повідомлень і дзвінків?

– Чи встановлені на наданих на дослідження об'єктах програми (клієнти) для дистанційного банківського обслуговування на зразок «Клієнт-Банк», «Інтернет-Банкінг»? Якщо так, чи містять вони log-файли використання зазначених програм?

– Чи наявні у наданому на дослідження відеореєстратори відеозаписи, створені в період (зазначити дату й час необхідних відеозаписів)? Якщо так, то виявлені відеозаписи скопіювати на окремий носій.

– Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої, і як ці несправності впливають на роботу обладнання в цілому?

– Чи можливе виконання (зазначити конкретні дії, наприклад: віддалене керування комп'ютером) дій за допомогою програмного (зазначити перелік програмних продуктів) продукту?

– Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розроблення?

– Які ігрові програми містяться в пам'яті наданих апаратів?

– Яка статистична інформація про ввід та вивід ігрових одиниць міститься в пам'яті наданих апаратів?

– Чи містяться на жорстких дисках обладнання програми-емулятори гри, якщо так, то які саме? Яка інформація міститься в протоколах (log-файлах) роботи програм?

– Встановити історію відвідування Інтернету за певний період.

– Чи міститься на жорстких дисках інформація про відвідування відповідних Інтернет-сайтів (зазначити, яких саме)?

– Чи містяться на наданих на дослідження об'єктах наявні та видалені файли документів формату «doc», «docx», «pdf» та електронних таблиць формату «xls», «xlsx»?

– Чи міститься на наданих на дослідження об'єктах серед наявних і видалених файлів інформація про ключові слова чи словосполучення (зазначити, які саме)? Якщо так, то які атрибути (дата й час створення, редагування, друкування, видалення тощо) файлів, що містять цю інформацію?

– Чи містяться на наданих на дослідження об'єктах файли листів електронної пошти? У разі наявності скопіювати зазначену інформацію на окремий носій.

– До яких веб-адрес Інтернету та коли здійснювали доступ з наданих на дослідження об'єктів (зазвичай зазначається перелік конкретних веб-ресурсів)?

– Чи містяться на наданих на дослідження об'єктах облікові дані (логіни та паролі) для доступу до Інтернет-ресурсів?

– Чи міститься на жорстких дисках системних блоків програмне забезпечення для прийняття ставок на спортивні події, бази

даних, якщо так то яка саме інформація міститься на жорстких дисках?

– Чи встановлені на жорстких дисках системних блоків драйвера для принтерів ... (перераховуються принтери, якими друкували квитанції)?

– Чи можливо за допомогою наданих на дослідження пристроїв проводити гру з можливістю виграшу, обов'язковою умовою участі в якій є внесення коштів[57]?

– Чи містяться на наданих на дослідження об'єктах серед наявної та видаленої інформації графічні або відеофайли з ознаками порнографічної продукції? (Виключно в разі призначення комплексної комп'ютерно-технічної та мистецтвознавчої судової експертизи)[58].

Зазначений перелік питань не є вичерпним і може бути конкретизований та уточнений у залежності від завдань (ідентифікаційних або діагностичних), які ставляться перед експертом у конкретному кримінальному провадженні Зокрема, лише в рамках дослідження маніпуляцій з браузером можна ставити питання про те, чи звертався користувач до певного браузеру, зокрема спеціальних браузерів, що дають змогу приховати користувача (наприклад, TOR); які сайти відвідував користувач; чи здійснював він там певні маніпуляції; чи є можливим, що «слід» користувача в браузері був сфабрикований задля приховання злочину[59].

---

[57] Інструкція про призначення та проведення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98. (дата звернення: 03.02.2021); Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 27; Довженко О. Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету*. *Серія: Право.* Вип. 55. Т. 2. С. 126.

[58] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 27.

[59] Полякова М. В., Рукавішников В. С., Шабля О. М. Особливості експертних досліджень файлових структур, типових для функціонування окремих інтернет-браузерів. *Теорія та практика судової експертизи і криміналістики.* 2014. Вип. 10. С. 528.

Предмет СКТЕ складають закономірності формування і дослідження комп'ютерних систем і руху комп'ютерної інформації, факти і обставини, що встановлюються на основі дослідження закономірностей розробки й експлуатації комп'ютерних засобів, які забезпечують реалізацію інформаційних процесів, котрі зафіксовані в матеріалах кримінального провадження[60].

Об'єктом СКТЕ є комп'ютерна техніка (ноутбуки, нетбуки, планшети тощо), периферійні пристрої (модеми, сканери, принтери, плотери, дисплеї, дисководи, клавіатури, маніпулятори тощо), мережеві апаратні засоби (мережеві кабелі, робочі станції, сервери), різноманітні носії інформації (магнітні, оптомагнітні, лазерні та ін.), програмне забезпечення, інша інформація, що знаходиться на носіях і в запам'ятовуючих пристроях (постійних та оперативних), а також органайзери, пейджери, мобільні телефони та інші прилади, що виготовлені та працюють на основі технологій побудови персональної комп'ютерної техніки; програми та програмні засоби, їх компоненти (підсистеми) та супроводжуючі аналітичні матеріали й технічні документи (словники пошукових ознак систем (тезауруси), технічні завдання і звіти, класифікатори, вимоги, специфікації, моделі та ін.), алгоритми, окремі програмні модулі, вихідні тексти програм, текстові та графічні документи (в електронній формі), дані в форматах мультимедіа, виготовлені з використанням комп'ютерних засобів; роздруківка програмних і текстових файлів; інформація у форматах баз даних, журнали (протоколи) роботи спеціалізованих програм, інших додатків прикладного характеру, інформаційні дані; електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них; інформація, розміщена на сайтах в мережі Інтернет. Важливо зазначити, що модеми та пристрої, що підтримують роботу комп'ютерних мереж (свічі, хаби тощо) не виділяються в окрему категорію, а включаються у визначення «комп'ютерна техніка».

Найчастіше об'єкти експертизи, що розглядається, є засобами вчинення злочинів (підробка документів, ухилення від сплати

[60] Незалежний інститут судових експертиз. Офіційний сайт. URL: https://nise.com.ua/it-ekspertyza (дата звернення: 03.02.2021); Експертизи у судочинстві України : науково-практичний посібник / заг. ред. В. Г. Гончаренка, І. В. Гори. К. : Юрінком Інтер, 2014. С. 118-119.

податків, виготовлення фальшивих грошей, приховування слідів злочину тощо). Однак не менш поширеними є злочини, при вчиненні яких об'єктом посягання стає інформація, що знаходиться в комп'ютері, на якому-небудь носії, чи саме програмне забезпечення. Крім того магнітні носії комп'ютерів нерідко є місцем зберігання чи навіть приховування інформації, що становить інтерес для досудового розслідування злочину (у певних випадках комп'ютер або комп'ютерна мережа досліджуються як середовище, в якому вчинені певні дії)[61].

Отже, відносно процесу розслідування сукупність зазначених об'єктів може розглядатись як знаряддя злочину та як носії слідів злочину[62]. Усі зазначені об'єкти СКТЕ для зручності можна умовно поділити на три класи – клас апаратних об'єктів, клас програмних та клас інформаційних об'єктів (даних)[63].

[61] Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).

[62] Коршенко В. А. Проблема визначення об'єктів судової комп'ютерно-технічної експертизи. *Вісник Харківського національного університету внутрішніх справ*. 2000. С. 151.

[63] Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук: 12.00.09. К., 2008. С. 88.

4 ДІЯЛЬНІСТЬ СЛІДЧОГО, ПРОКУРОРА ЩОДО ЗАЛУЧЕННЯ ЕКСПЕРТА ДО ПРОВЕДЕННЯ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Залучення експерта до процесу розслідування кримінального правопорушення здійснюється, насамперед, у процесі проведення судової експертизи, яка є процесом діяльності обізнаної особи, здійснення дослідження, і потребує звернення до спеціальних знань[64].

Закон України «Про судову експертизу» визначає судову експертизу, як дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо, об'єктів, явищ і процесів із метою надання висновку з питань, що є або будуть предметом судового розгляду (ст. 1)[65]. Судова експертиза є важливою, найбільш досконалою та результативною формою використання спеціальних знань у кримінальному провадженні, сутність якої полягає в аналізі обізнаною особою – експертом наданих у його розпорядження уповноваженими суб'єктами матеріальних об'єктів (речових доказів), а також різних документів (у тому числі, у електронному вигляді) з метою встановлення фактичних даних, що мають значення для правильного вирішення кримінального провадження.

Судову експертизу як самостійну форму застосування спеціальних знань в кримінальному судочинстві характеризує сукупність наступних ознак: особлива процесуальна форма дослідження; значимість встановлюваного обставини для справи; здійснення

[64] Шепітько В. Ю., Журавель В. А., Авдеева Г. К. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : монографія. Х. : Вид. агенція «Апостіль», 2017. С. 118.

[65] Про судову експертизу: Закон України від 25.02.1994 р. № 4038-XII. Відомості Верховної Ради України. URL: http://zakon2.rada.gov.ua/laws/show/4038-12 (дата звернення: 03.02.2021).

досліджень експертом як компетентним спеціалістом; оформлення результатів у формі висновку експерта, який є одним із передбачених законом джерел доказів.

У процесі досудового розслідування об'єм використання можливостей судової експертизи визначається низкою чинників: змістом та особливостями доказування у провадженнях за певним видом злочинів; загальними вимогами кримінального процесуального закону, що встановлюють коло обставин, для встановлення яких призначення та проведення судових експертиз є обов'язковим; змістом конкретних доказових фактів, встановлення яких можливе завдяки проведенню судових експертиз на певному етапі досудового розслідування в конкретних слідчих ситуаціях; типовими та індивідуальними характеристиками об'єктів судово-експертних досліджень; реальними можливостями судово-експертних установ із проведення експертиз певного виду; рівнем професійної підготовки посадових осіб, які здійснюють кримінальне провадження[66].

Беззаперечним є те, що експертиза відіграє значну роль у розслідуванні великої кількості злочинів. Особливо важливою вона стає для розслідування тих із них, які вчинюються за допомогою можливостей комп'ютерної техніки та Інтернет-мережі. Особа, яка вчинює кримінальне правопорушення, зазвичай, на високому рівні орієнтується в галузі комп'ютерної техніки, отже, для розслідування його дій необхідні експертні знання, що не поступаються знанням зловмисника.

Основні організаційно-тактичні рекомендації щодо призначення судової експертизи у кримінальному провадженні достатньо успішно розроблені криміналістичною наукою і апробовані слідчо-експертною практикою. Разом з тим вважаємо, що процедура призначення судової експертизи носить комплексний характер і повинна враховувати тактико-організаційні, кримінально-процесуальні та психологічні аспекти.

В Україні питання проведення експертиз регламентовано Інструкцією про призначення та проведення судових експертиз та експертних досліджень, а також Науково-методичними рекоменда-

[66] Бондар В. С., Солодовніков А. П, Дехтярьов Є. В. Розслідування розбоїв, вчинених організованими групами : навч.-метод. посібник. 2014. С. 22.

ціями з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених Наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5[67]. Інструкція поряд з електротехнічною та телекомунікаційною, вказує комп'ютерно-технічну експертизу, як різновид інженерно-технічної експертизи.

СКТЕ під час досудового розслідування зазвичай призначається на його початковому етапі, після проведення огляду місця події та обшуку, коли інформації для подальшого розслідування недостатньо. СКТЕ – це самостійний рід судових експертиз, що відноситься до класу інженерно-технічних і проводиться з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення й вивчення його слідової картини, а також отримання доступу до інформації на носіях з подальшим всебічним її дослідженням[68].

Під час досудового розслідування слідчий, прокурор може дійти переконання про необхідність призначення СКТЕ об'єктів, знайдених та (або) вилучених під час виконання огляду, обшуку, інших процесуальних дій. Найчастіше об'єкти СКТЕ є засобами вчинення кримінальних правопорушень (ухилення від сплати податків, підробка документів, виготовлення, зберігання придбання, перевезення, пересилання підроблених грошей тощо). Поширеними є й кримінальні правопорушення, при вчиненні яких об'єктом посягання стає інформація, що міститься в комп'ютері, на певному носії, чи саме програмне забезпечення. Крім того магнітні носії комп'ютерів нерідко є місцем зберігання, приховування інформації, що становить інтерес для правоохоронних органів[69].

Якщо говорити про діяльність слідчого (прокурора) щодо залучення експерта до проведення СКТЕ у кримінальному провадженні, то вона визначається *комплексом його дій*, а саме: прийнят-

---

[67] Інструкція про призначення та проведення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 03.02.2021).

[68] Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук: 12.00.09. К., 2008. С. 78.

[69] Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).

тя рішення про проведення експертизи; формулювання запитань на вирішення експерта; визначення матеріалів кримінального провадження, що містять вихідні дані для експертизи; вибір експертної установи і експерта; відбір і підготовка об'єктів дослідження і порівняльних матеріалів (зразків); ділова взаємодія слідчого і експерта (комісії експертів) в процесі підготовки і призначення експертизи.

Саме такою послідовністю дій повинен послуговуватись слідчий, прокурор у разі, коли прийде до переконання щодо необхідності призначення СКТЕ у кримінальному провадженні. З огляду на предмет дослідження конкретизуємо такий алгоритм дій.

Прийняття рішення про проведення експертизи.

За змістом ст. 242 КПК України, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання, під час досудового розслідування експертиза може бути проведена експертною установою, експертом або експертами, у тому числі за ініціативи слідчого, прокурора, як представників сторони обвинувачення у кримінальному провадженні.

Доводиться констатувати наявність певних упущень і у цій сфері діяльності. Так, у справі № 161/11495/18 прокурор у клопотанні про проведення комп'ютерно-технічної експертизи, з яким звернувся до Луцького міськрайонного суду Волинської області, не виконав вимоги п. 3 ч. 2 ст. 244 КПК України, а саме, не виклав обставин, якими обґрунтовуються доводи клопотання про проведення саме комп'ютерно-технічної експертизи, не мотивував вид експертного дослідження, який необхідно провести. З огляду на це, слідчим суддею у задоволенні вказаного клопотання було відмовлено[70].

Відповідно до ч. 3 ст. 244 КПК України, особа, яка подала клопотання, повідомляється про місце та час його розгляду, проте її неприбуття не перешкоджає розгляду клопотання, крім випадків, коли її участь визнана слідчим суддею обов'язковою. Враховуючи те, що учасник процесуальної дії не з'явився в судове засідання, слідчий суддя може розглянути клопотання без застосування

[70] Ухвала слідчого судді Луцького міськрайонного суду Волинської області про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 26.07.2018 у справі № 161/11495/18 (кримінальне провадження № 1-кс/161/6086/18). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

технічних засобів фіксування та прийняти рішення про доцільність призначення судової комп'ютерно-технічної експертизи[71].

Інформація, відображена у постанові про призначення СКТЕ, повинна включати короткий виклад обставин кримінального провадження, правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність, виклад обставин, якими обґрунтовуються доводи ініціатора, вид експертного дослідження, яке необхідно провести, а також перелік питань, які необхідно поставити експерту (див. Додаток А).

Формулювання запитань на вирішення експерта

Орієнтовний перелік запитань, які ставляться на вирішення експерта при призначенні СКТЕ нами було наведено у попередньому розділі. Тому зосередимо увагу на організаційних аспектах цього питання.

Однією з практичних проблем, пов'язаних з проведенням судових експертиз при розслідуванні корупційних діянь, є їх тривалість, що призводить до невиправданого затягування строків вирішення таких кримінальних проваджень по суті. На тривалість перебування матеріалів кримінальних проваджень у експертній установі іноді впливає некоректне формулювання в ухвалах про доручення проведення експертизи переліку питань, які ставляться на вирішення експерта[72].

Необхідно підкреслити, що кожен з кіберзлочинів має свої особливості та вимагає спеціального підходу, а характер злочинів постійно змінюється. Поділяємо точку зору О.Ю. Довженко, що методологічно коректнішим було б складання рекомендацій до самого процесу постановки запитань, що дало б змогу слідчому формулювати їх максимально коректно. Зокрема, слід визначити такі моменти. По-перше, питання не повинні бути правовими (на-

[71] Ухвала слідчого судді Рівненського міського суду Рівненської області про призначення судової комп'ютерно-технічної експертизи від 13.12.2018 у справі № 569/23518/18 (кримінальне провадження № 12018180010002477). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

[72] Климчук М. П., Михайлов П. С. Судова комп'ютерно-технічна експертиза як спосіб виявлення корупційної складової при розслідуванні протиправного впливу на результати офіційних спортивних змагань. *Вчені записки ТНУ імені В. І. Вернадського.* 2020. Т. 31 (70). Ч. 3. № 2. С. 109.

приклад, чи є об'єкт дослідження контрафактним), торкатися вартості об'єкта дослідження (наприклад, якою є вартість об'єкта дослідження), перекладу тексту, листування тощо. По-друге, питання повинні мати технічний характер (наприклад, якою є загальна характеристика представленого програмного забезпечення, з яких компонент (програмних засобів) воно складається). Також питання може стосуватися роз'яснення жаргонізмів та комп'ютерних термінів. По-третє, питання повинні бути складені з огляду на завдання дослідження (ідентифікаційні або діагностичні).

В деяких випадках, якщо експертиза потребує вирішення більш детальних питань про встановлення фактів та способів передачі (отримання) інформації в глобальній мережі Інтернет, або необхідно провести дослідження алгоритмів обробки інформації виявленого шкідливого програмного забезпечення на об'єкті дослідження, то в такому разі необхідно вирішити питання про призначення комплексної СКТЕ, а також експертизи телекомунікаційних систем та засобів.

Для складання коректного переліку питань для комп'ютерно-технічної експертизи слідчому необхідно узгодити складені ним питання з фахівцем або звернутися за допомогою до фахівця й скласти питання разом з ним[73].

Важливим критерієм повноти та глибини висновку експерта є не лише подання йому усіх необхідних матеріалів для дослідження, а й постановка чітких запитань на вирішення експерта. Яка, на жаль, нерідко констатується учасниками кримінального провадження. Так, слідчий суддя Октябрського районного суду м. Полтави залишив без виконання комп'ютерно-технічну експертизу у кримінальному провадженні № 42019171010000004, оскільки експертом, в ході дослідження, було встановлено низку суттєвих недоліків які унеможливлюють об'єктивне проведення експертизи[74].

---

[73] Довженко О. Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету. Серія: Право.* Вип. 55. Т. 2. С. 126.

[74] Ухвала слідчого судді Октябрського районного суду м. Полтави від 26.03.2019 у справі № 569/1173/19 (кримінальне провадження № 42019171010000004). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

За слушним зауваженням П. П. Харківського, з методичних посібників чи затверджених наказом Міністерства юстиції методичних рекомендацій нерідко слідчому важко визначити, які саме зі вказаних питань слід поставити на розгляд експерта. Нестача знань й неповне розуміння слідчим сутності проблеми, що підлягає дослідженню, може приводити до винесення на розгляд експерта питань, що не стосуються злочину безпосередньо. Зрештою, це приводить до затягування розслідування та зниження його ефективності[75].

При цьому слід зазначити, що експерт не має права самостійно збирати матеріали, які підлягають дослідженню, а також вибирати вихідні дані для проведення експертизи, якщо вони відображені у наданих йому матеріалах неоднозначно. Слід дуже уважно ставитися до питань, що задаються експерту, і за можливості конкретизувати їх. Приміром, Новозаводський районний суд Чернігівської області ухвалою від 18.12.2015 року відмовив у призначенні комплексної комп'ютерно-технічної експертизи з тих підстав, що питання, поставлені на вирішення експерта, є дуже узагальненими та не можуть бути у такому вигляді поставлені на вирішення навіть комплексної експертизи[76].

Вважаємо доцільним перед призначенням СКТЕ звернення до спеціаліста з приводу уточнення, складання коректного переліку питань, які можуть бути вирішені при проведенні експертизи у конкретному кримінальному провадженні. Адже, як слушно зазначає Б. Б. Теплицький, ні слідчий, ні оперативний працівник з об'єктивних причин не можуть бути носіями таких спеціальних знань і навичок, а отже, не можуть ефективно провадити свою діяльність із виявлення та розкриття злочинів відповідної категорії без участі фахівця-носія таких спеціальних знань і навичок[77].

---

[75] Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2 (22). С. 98.

[76] Ухвала слідчого судді Новозаводського районного суду Чернігівської області про відмову у призначенні комплексної комп'ютерно-технічної експертизи від 18.12.2015 у справі № 751/6804/18. URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

[77] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 28.

При призначенні судової експертизи, пов'язаної з дослідженням електронної слідової інформації, спеціаліст може: звернути увагу на помилки в збиранні (виявленні, фіксації, вилученні) цифрових слідів, що впливають в подальшому на висновки експертів (придатність або непридатність об'єктів); уточнити рід або вид СКТЕ або іншої експертизи, уточнити, чи буде вона моно- або комплексною; допомогти визначитись з вибором експертної установи або кандидатури експерта; надати допомогу у формулюванні запитань експерту; вказати на неможливість вирішення питання через відсутність експертної методики, недостатнього рівня розвитку науки і технології; вказати на неприпустимість постановки деяких запитань, що виходять за межі компетенції експерта або не потребують використання спеціальних знань; вказати на матеріали, які необхідно надати в розпорядження експерта.

Відбір і підготовка об'єктів дослідження і порівняльних матеріалів (зразків).

Необхідно також зазначити, що перед призначенням СКТЕ слідчий повинен підготувати відомості й матеріали щодо стосуються її предмета. Зокрема, слід оцінити та перевірити достатність об'єктів для проведення експертизи, оформити їх для подальшої передачі до експертної установи. Чітке визначення технічних та якісних характеристик наданого на дослідження об'єкта однозначно ідентифікує його. Зазначена вимога не є суто технічною, адже вона може мати велике значення під час визначення допустимості об'єкта, порушення якого може породити непереборні сумніви щодо автентичності, й надалі дасть усі підстави тлумачити такий висновок експерта як недопустимий доказ[78].

Важливим під час оформлення об'єктів для проведення експертизи, у т. ч. СКТЕ, є їхнє пакування. Якщо це зовнішній носій інформації, його необхідно упакувати й опечатати по місцях відкриття упаковки. Якщо це внутрішній носій інформації, який є частиною спецтехніки, його за можливості необхідно відокремити від техніки й також підготувати до передачі експерту або передати разом з обладнанням, яке слід упакувати.

[78] Орлов Ю. К. Судебная экспертиза как средство доказывания в уголовном судопроизводстве : науч. изд. М. : Институт повышения квалификации РФЦСЭ при Минюсте России, 2005. С. 140.

У разі необхідності отримання зразків для проведення експертизи вони відбираються стороною кримінального провадження, яка звернулася за проведенням експертизи або за клопотанням якої експертиза призначена слідчим суддею[79]. Отже, слідчий суддя при призначенні експертизи має право тільки вирішити питання про отримання зразків для експертизи і не має права надавати експерту дозвіл на користування своїми правами та виконання своїх обов'язків, визначених ст. 69 КПК України. За таких обставин, слідчий суддя Сєвєродонецького міського суду Луганської області визнав за необхідне частково відмовити у задоволенні клопотання слідчого про призначення судової комп'ютерно-технічної експертизи в частині надання дозволу на виконання вимог ст. 69 КПК України[80].

У випадку, якщо проведення експертизи доручено судом, відібрання зразків для її проведення здійснюється судом або за його дорученням залученим спеціалістом (ч. 1 ст. 245 КПК України).

Оформлення відібраних зразків й матеріалів здійснюється відповідно до положень КПК України. Приміром, для дослідження інформації, яка міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби – комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій). Для збереження даних на досліджуваних носіях вони надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в таких пакуваннях, що роблять неможливим доступ до носіїв інформації безпосередньо чи підключення системного блоку до мережі живлення. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду. Для дослідження робочого стану комп'ютерно-

[79] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

[80] Ухвала слідчого судді Сєвєродонецького міського суду Луганської області про призначення судової комп'ютерно технічної експертизи від 22.03.2019 у справі № 428/3245/19 (кримінальне провадження № 12018130370002160). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них. Задля визначення того, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки[81].

Науковцями неодноразово вказувалось, що відсутність чітких уявлень про предмет експертизи, її видовий розподіл, застаріла класифікація об'єктів експертизи тощо перешкоджають системній розробці методів експертного дослідження, налагодженню активної взаємодії між підрозділами, які проводять досудове розслідування злочинів[82].

При розслідуванні кримінальних правопорушень, пов'язаних з використанням комп'ютерної техніки, некваліфіковані дії дозволяють засумніватися у відсутності модифікації інформації на магнітному диску, а також можуть призвести до її видалення. Регулярно помічалося, що вилучений комп'ютер включався співробітниками оперативних і слідчих підрозділів, які намагались виявити електронну інформацію, що відноситься до розпочатого кримінального провадження, а іноді здійснювали набір і роздруківку службових документів в редакторі, пошук інформації в Інтернет та ін. Природно, у зв'язку із «постійною нестачею часу» не здійснювалося протоколювання даних дій, які впливали на зміну інформації речового доказу. Хоча давно відомо, що навіть відкриття і перегляд наявних файлів, а тим більше створення нових текстів і встановлення програмного забезпечення модифікують службову й іншу інформацію на накопичувачі і не дозволяють в подальшому провести експертизу через неможливість відновлення існуючих віддалених файлів.

При вилученні елементів комп'ютерної техніки часто опечатування не запобігає можливості підключення носія електронної інформації до електричної мережі або до іншого пристрою, що

[81] Інструкція про призначення та проведення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 03.02.2021).

[82] Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2 (22). С. 98.

дозволяє засумніватися в незмінності і відсутності модифікації інформації речового доказу, здійсненої як навмисне, так і без наміру. Оскільки навіть звичайне відключення системного блоку із завантаженням операційної системи призводить до створення нових файлів службового призначення. При завантаженні операційних систем створюється спеціальний файл підкачки, який розширює віртуальну пам'ять, створюються резервні копії файлів реєстру і вносяться інші зміни на накопичувач електронної інформації. Запущені програми створюють спеціальні тимчасові файли для резервного копіювання та фіксації модифікацій редагованого електронного документа. Відкриття електронних документів, запуск програмних продуктів і навігація по сайтах Інтернету викликає модифікацію службових файлів операційної системи, залишає сліди в історії роботи, папках, що містять тимчасові і log-файли, а також спеціальних папках, що містять сліди роботи в Інтернеті. При створенні або копіюванні на носій зовнішньої пам'яті нових файлів змінюється інформація в кластерах, зазначених операційною системою як вільна або невживана, яка може містити видалені файли. Дані процеси записують нову інформацію поверх існуючих раніше видалених електронних документів, які можливо було відновити і завдяки ним відтворити криміналістично важливі сліди, що сприяють розслідуванню розглянутих кримінальних правопорушень[83]. І навіть якщо такої модифікації не виявлено, то перше питання експертизи про можливість підключення даної техніки має позитивну відповідь, що ставить під сумнів легітимність даного речового доказу.

Причиною процесуальних, методичних, логічних помилок, упущень, прорахунків можуть бути некваліфіковані дії оперативних та слідчих підрозділів, відсутність належної комунікації між слідчим та експертом. Їх своєчасне виявлення та виправлення сприятиме підвищенню якості СКТЕ, відповідності висновків експерта поставленим запитанням.

Під час досудового розслідування слідчому, прокурору, суду слід переконатися в тому, що поставлене завдання може бути

[83] Костин П. В., Кувычков С. И. Исследование магнитных носителей : учебное пособие. Н. Новгород, 2002. С. 22–26.

розв'язане експертом в рамках призначеної експертизи, чи забезпечений експерт достатнім обсягом матеріалів, доказів та об'єктів дослідження, які необхідні йому для повного та всебічного дослідження й відповіді на поставлені запитання[84]. Отже, не менш важливим видається визначення *компетенції та компетентності* експерта, якому доручається проведення СКТЕ.

Компетенція експерта (від лат. *compete* – відповідати, бути придатним) О. Р. Росинською розглядається у двох аспектах. По-перше (у правовому) значені, як коло повноважень, прав і обов'язків експерта, які визначені процесуальними кодексами і відомчими нормативними актами. По-друге в науковому аспекті, як комплекс спеціальних знань у сфері теорії, методики і практики певного роду, виду експертизи[85].

Компетентність – це головна вимога до особи, яка залучається до проведення судової експертизи, незалежно від її професійного статусу. Компетентний (від лат. *competcns (competentis)* – «який має достатні знання в якій-небудь галузі, який з чим-небудь добре обізнаний».

Хоча природа експертних помилок різна, в основі кожної з них лежить недостатня компетентність експерта. Компетентність відображає готовність експерта до практичного провадження експертних досліджень. Вона складається зі знань в галузі фундаментальної для кожного роду експертиз науки, наукових основ і процесуальної регламентації судової експертизи і знання експертних методик. Кожен із зазначених компонентів впливає на якість експертного дослідження[86].

На слушне зауваження окремих науковців, зазначення слідчим того чи іншого різновиду СКТЕ може створити зайві складнощі під час проведення експертизи чи відповідей на окремі питання,

---

[84] Степанов В. В., Бабаков М. А. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий. М. : Юрлитинформ, 2014. С. 35.

[85] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. 2-е изд., перераб. и доп. М. : Норма, 2008. С. 27.

[86] Рувін О.Г. Судові експертизи в процесуальному праві України : навч. посіб. К. : Вид-во Ліра-К, 2019. С. 208.

які підлягають вирішенню[87]. Слідчому достатньо відзначити рід експертизи, а експерт, проаналізувавши питання й оцінивши об'єкти, сам визначить конкретний вид експертизи[88].

Як зазначається у Інструкції про призначення та проведення судових експертиз, видом експертизи є інженерно-технічна, а підвидом – комп'ютерно-технічна. Тобто під час призначення експертизи може вказуватись лише інженерно-технічна експертиза (вид) та комп'ютерно-технічна (підвид). Отже, до компетенції слідчого належить лише визначення виду експертизи, а конкретний експерт, якому вона буде доручена, визначається керівником експертної установи.

[87] Менжега М. М. Криминалистические проблемы расследования создания использования и распространения вредоносных программ для ЭВМ : дисс. … канд. юрид. наук. Саратов, 2005. С. 122.

[88] Поляков В. В., Шебалин А. В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации. Барнаул, 2013. С. 85.

5 МЕТОДИКА ПРОВЕДЕННЯ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Будь-яке експертне дослідження ґрунтується на методиках проведення експертиз різних класів, родів і видів і являє собою систему пізнавальних засобів, що визначають зміст і структуру дослідження. Ці методики є результатом спеціальних наукових розробок. Звісно, що в даний час повинні розроблятись такі рекомендації не тільки з підвищення якості діяльності слідчих, прокурорів, співробітників оперативних служб, а й судових експертів та спеціалістів. При цьому особливої уваги заслуговує вирішення проблем забезпечення якості основного результату діяльності експерта – висновку експерта, який сприяє встановленню обставин, які підлягають доказуванню у кримінальному провадженні (ст. 91 КПК України), і визнаний законодавцем джерелом доказів у ньому (ч. 2 ст. 84 КПК).

Завдання, які вирішуються експертом, можуть бути типовими, стандартними і творчими (евристичними), вимагати нестандартного підходу, розробки нової або модернізації діючої методики. Якщо завдання типове і вирішується за допомогою стандартної методики, то вона піддається алгоритмізації, що формалізує процес експертного дослідження. Евристичне завдання вимагає від експерта високої кваліфікації, досконалого володіння методиками, вміння знаходити нестандартне його вирішення. Таким чином, пізнавальна діяльність експерта являє собою співвідношення творчого початку і стандартності, залежить від наукового рівня розроблених методик і методів вирішення завдань експертизи певного роду і виду[89].

В ідеалі для дослідження кожного виду об'єктів під час проведення судової експертизи повинна існувати система категорич-

[89] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи. *Судебная экспертиза.* М. : Проспект, 2010. С. 214.

них або альтернативних науково обґрунтованих рекомендацій щодо вибору та застосування в відповідної послідовності, а також методів, прийомів і засобів, що існують або створюються в певних умовах (пристроїв, приладів і апаратури) для вирішення експертного завдання. Категоричний або альтернативний характер методики, тобто відсутність або наявність у експерта можливості вибору, залежить від сутності обраних методів і засобів.

На сучасному рівні розвитку судової експертології повна стандартизація і алгоритмізація всього процесу експертного дослідження неможливі. Завданням експерта завжди буде початковий аналіз вихідних даних (проблемна ситуація) і осмислення результатів проведених досліджень перед формулюванням остаточного висновку, навіть якщо саме дослідження здійснювалося за стандартною методикою з високим рівнем програмування діяльності експерта на етапі власне дослідження об'єкта. Методика містить рекомендації та обов'язкові правила з ключових моментів, що визначає схему дослідження. Весь зміст конкретного експертного дослідження не може передбачити жодна методика. Тому, творчі компоненти зазвичай присутні в кожному експертному дослідженні[90].

Розслідування кримінальних правопорушень, вчинених з використанням комп'ютерної техніки та комп'ютерних технологій, проведення судових експертиз по них ускладнюється тим, що з постійним розвитком інформаційних технологій з'являються об'єкти дослідження, яких раніше не існувало, постійно змінюються, модифікуються механізми і методи вчинення раніше відомих видів злочинів, з'являються абсолютно їх нові види[91]. Експертам для дачі повного, достовірного, науково обґрунтованого висновку необхідне постійне підвищення кваліфікації, вдосконалення навичок, оновлення наявних знань і використання методичної літератури, що відповідає вимогам сьогодення.

Зміст експертних методичних підходів СКТЕ визначається, насамперед метою і завданнями даного роду судових експертиз.

---

[90] Россинская Е. Н. Гносеологические и деятельностные экспертные ошибки при использовании в производстве судебных экспертиз современных технологий. *Вестник Московского университета МВД России*. № 3/2015. С. 19.

[91] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. *Право и закон.* М., 2001. С. 15.

Вимоги до методичного забезпечення СКТЕ базуються на основних процесуальних нормах, визначених КПК України стосовно судової експертизи, а також положеннях Закону України «Про судову експертизу» № 4038-XII від 25 лютого 1994 р. Сучасне вітчизняне судочинство висуває такі вимоги до СКТЕ: законність, обґрунтованість, достовірність отриманих результатів, безпека, ефективність, економічність, етичність, допустимість. Експерт у своїй діяльності має виходити з таких загальних положень: об'єктивності, повноти та всебічності дослідження; його своєчасності; цілеспрямованості і плановості; безпосередності дослідження об'єктів експертизи; процесуального оформлення її результатів[92].

При дослідженні нових, таких що не часто трапляються об'єктів, експерти керуються методиками, розробленими науковцями інших галузей знань й опублікованими в спеціальній літературі. Не дивлячись на те, що такі методики ґрунтуються на загальноприйнятих в цих галузях наукових принципах, вони не є однозначними й еквівалентними, припускають варіативність підходів, можуть ґрунтуватися на різних наукових поглядах, галузевій специфіці, різного ступеню адаптації зарубіжних методик до вітчизняної практики. Також при проведенні СКТЕ не є можливим застосування певних припущень, ймовірнісних підходів, що ґрунтуються лише на наукових теоріях окремих авторів або навіть на окремих гіпотезах. Такі висновки експерта не можуть визнаватися достовірними й допустимими й не можуть підвищувати ступінь достатності доказів у кримінальному провадженні[93].

В результаті аналізу низки методик проведення СКТЕ ми дійшли висновку, що окремі з них не відповідають усьому комплексу вимог законодавства України; деякі практикують популяризаторський підхід; частина з них містить смислові помилки. Розробка уніфікованої методики проведення СКТЕ, яка б відповідала вимогам законодавства та сьогодення, враховувала навички вітчизняних та зарубіжних авторів, в даний час є актуальною та необхідною.

---

[92] Шепітько В. Ю., Коновалова В. О., Журавель В. А. Криміналістика: підручник: 4-е вид., перероб. і доп. Х. : Право, 2010. С. 266.

[93] Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1 (9). С. 143.

З метою об'єктивізації результатів методик СКТЕ, уніфікації підходів до їх формування необхідно виходити з принципів однакового підходу до структури методики[94], яка повинна відповідати сучасному рівню розвитку науки і техніки, вимогам вітчизняного законодавства та, водночас, може бути ефективною при проведенні СКТЕ з практично будь-яких питань даного роду експертизи.

На переконання В. А. Коршенко, методика дослідження повинна містити в собі: алгоритм дій експерта під час проведення дослідження з розв'язання типових завдань; рекомендації з вибору джерел інформації (технічної літератури, довідкових видань, електронні форуми з вказаних питань тощо); рекомендації з вибору програмного забезпечення для проведення експертизи; рекомендації з технічного забезпечення експерта[95]. Поділяємо точку зору Е. Б. Сімакової-Єфремян, що у кожній з методик обов'язковою повинна бути наявність таких компонентів: предмет, задачі, об'єкти й суб'єкти дослідження, застосовувані методи, викладення алгоритму послідовності дій експерта й оцінки отриманих результатів. Окрім цих обов'язкових складових, методика експертного дослідження може містити й рекомендації з підготовки матеріалів для проведення експертиз або оцінки отриманих результатів[96].

Очевидним є те, що при проведенні експертизи слідчому, прокурору, судді, зазвичай, не під силу в повній мірі розібратися в доцільності (як власне, й науковості і допустимості) використання певного методу або методики, попри наявні в літературі численні запевнення про зворотне. З огляду на це, зазначений розділ адресований, насамперед, експертам.

---

[94] Сімакова-Єфремян Е. Б., Балинян Т. Є., Дереча Л. М. Про критерії оцінювання методик проведення судових експертиз в Україні. Теорія та практика судової експертизи і криміналістики : зб. наук. праць. 2010. Вип. 10. Х. : Право, 2010. С. 151-156.

[95] Коршенко В. А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jumalul juridic national: teorie i practica*. 2017. № 2. С. 192.

[96] Сімакова-Єфремян Е. Б., Балинян Т. Є., Дереча Л. М. Про критерії оцінювання методик проведення судових експертиз в Україні. Теорія та практика судової експертизи і криміналістики : зб. наук. праць. 2010. Вип. 10. Х. : Право, 2010. С. 151-156.

У загальному сенсі під окремою методикою проведення експертизи розуміється сукупність окремих методів, які застосовуються за певним алгоритмом[97]. Алгоритм проведення СКТЕ вважаємо доцільним розподілити на окремі, послідовні стадії: 1) підготовчу; 2) аналітичну; 3) експериментальну; 4) синтезуючу; 5) результативну; 6) формування висновків.

Кожна із виокремлених стадій має певні особливості та потребує детального аналізу.

Основна мета *підготовчої стадії* – з'ясування експертом експертного завдання, досягнення якого при проведенні СКТЕ можливе шляхом виконання такої впорядкованої послідовності дій і методів: аналіз постанови (ухвали), розгляд зазначених у ній запитань; вивчення матеріалів кримінального провадження; зовнішній огляд і опис об'єктів, наданих на експертизу (огляд рекомендується супроводжувати фото-, відеозйомкою об'єктів при їх надходженні до експертної установи – в упаковці і без упаковки з метою фіксації зовнішніх ознак досліджуваних об'єктів); попередній аналіз інформаційного вмісту об'єктів з метою визначення придатності і достатності об'єктів[98]; визначення можливостей СКТЕ та досягнення кінцевого результату дослідження; вибір методів дослідження; аналіз застосовуваності технічної бази (програмного забезпечення, обладнання) експертної установи для вирішення конкретних поставлених завдань; визначення відповідності кваліфікації експерта, складності питань, що вирішуються СКТЕ у конкретному кримінальному провадженні.

На даній стадії здійснюється перегляд нормативних документів і законодавчих актів, висуваються робочі гіпотези, визначаються необхідні методи, прийоми і засоби дослідження, а також алгоритм їх застосування. У разі необхідності запитуються додаткові матеріали, вивчається спеціальна і довідкова література.

Доцільним є аналіз наявності серед раніше проведених аналогічних експертиз, та використання плану раніше проведених експертиз в якості шаблону. У разі відсутності таких експертиз

---

[97] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. *Право и закон.* М., 2001. С. 159.

[98] Шелупанов А. А., Смолина А. Р. Методика проведения подготовительной стадии исследования. Доклады ТУСУРа. 2016. Т. 19. № 1. С. 32.

виправданим вважаємо складення є складання індивідуального плану проведення експертизи.

Досить різнорідний перелік завдань і об'єктів СКТЕ об'єктивно обумовлює застосування широкого кола експертних методів і засобів, арсенал яких постійно збагачується новими приладами та апаратурою, розширюється за рахунок застосування нових методів дослідження речових доказів[99]. Тому, при оцінці методів на допустимість оцінюється наукова обґрунтованість і задоволення метода новітнім досягненням галузі сучасних наукових технологій. Суттєвим недоліком існуючих, науково обґрунтованих методів дослідження є їх невідповідність сучасному рівню розвитку інформаційних технологій, що робить безглуздим їх застосування на практиці. У цій ситуації набуває великого значення наукова спеціалізація, професійний рівень і особистий досвід експерта СКТЕ.

Перед тим, як застосувати той чи інший метод або обладнання, судовому експерту рекомендується провести всебічний аналіз засобів і методів проведення судової експертизи, досягти такого рівня знань своєї експертної спеціальності, який дає змогу виключити використання техніко-криміналістичних систем, що дають викривлений результат, і застосувати відповідний варіант технічного виконання поставлене завдання[100].

Наступною важливою вимогою, яка пред'являється до експертних методів, є ефективність. Використовувані експертом СКТЕ методи повинні дозволяти в оптимальні терміни з найбільшою продуктивністю вирішувати поставлені завдання дослідження. Методи повинні мати властивість рентабельності, тобто сумірності витрачених сил і засобів з цінністю отриманих результатів. Не можна не погодитися з тим, що дослідження, проведене в дуже короткий термін, при цьому дала повні, чіткі, ясні, наочні й доступні відпові-

---

[99] Россинская Е. Н. Гносеологические и деятельностные экспертные ошибки при использовании в производстве судебных экспертиз современных технологий. *Вестник Московского университета МВД России*. 2015. № 3. С. 19.

[100] Хомутов С. В. По вопросу различных подходов к оценке заключения эксперта. *Вестник Восточно-Сибирского института МВД России.* 2019. № 1 (88). С. 267.

ді на поставлені запитання, позбавлене недоліків у порівнянні із висновком, терміни дачі якого триваліші, хід дослідження не досить зрозумілий, ілюстрацій менше, відповіді на запитання розмиті. Така значна різниця у висновках зазвичай виникає через те, що не всі експерти мають необхідний інструментарій через його високу вартість і використовують у своїй практиці менш витратні методи дослідження (використовують безкоштовне обладнання, працюють за відсутності необхідних апаратних комплексів тощо). Непоодинокими є випадки, коли експерти не заявляють самовідвід і працюють з тим, що є.

Відповідно до засади безпосередності дослідження показань, речей і документів, суд досліджує докази безпосередньо (ч. 1 ст. 23 КПК України). Тому зазвичай в методичній літературі даються рекомендації застосовувати насамперед неруйнівні (недеструктивні) методи щодо речових доказів, як об'єктів СКТЕ. Застосування руйнівних або частково руйнівних методів має бути усвідомленим, виправданим конкретною метою і узгодженим з особою, яка призначила експертизу. Так, найчастіше, недосвідчені експерти проводять експертизу, наданих на дослідження персональних комп'ютерів, просто включивши їх, прямо на них відновлюють вилучені файли, попередньо встановивши свої програми для відновлення і при цьому не вважають, що об'єкт дослідження руйнується. Застосування неруйнівних методів в СКТЕ не самоціль і може бути неефективним в даному конкретному випадку, коли повну інформацію про об'єкт можна отримати тільки при його руйнуванні, наприклад, «зламавши» парольний захист. Однак, при виході нових гаджетів, з'являються і складніші системи захисту, що унеможливлюють такий «злам» захисних паролів. В такому разі, слід звернути увагу на отримання паролів захисту при проведенні вилучення техніки, що дозволить безперешкодно провести експертне дослідження. Виходячи із сказаного, можна дійти до думки, що «чим новіший пристрій, тим складніша система захисту».

Під час перевірки допустимості методів СКТЕ враховується також їх безпека для експерта, характер впливу на апаратний, програмний або інформаційний об'єкт дослідження, час отримання результатів.

Вибір або розробка методики дослідження комп'ютерних засобів і систем подекуди залежить не тільки від об'єкта, але й від

сформованої слідчої ситуації. Використання тільки неруйнівних методів (при відсутності необхідних апаратно-програмних засобів) може призвести до затягування термінів виконання СКТЕ і мати негативні наслідки для розслідування, а також для судового розгляду кримінальних проваджень.

Відповідно до п. 3 ч. 5 ст. 69 КПК України експерт зобов'язаний забезпечити збереження об'єкта експертизи. Отже, якщо експерт вбачатиме необхідність використання на певному етапі руйнуючих/частково руйнуючих методів дослідження, він повинен звернутись з відповідним клопотанням до особи, яка залучила експерта. Так, у кримінальному провадженні № 12019020130000019 до Жмеринського міськрайонного суду надійшло клопотання експерта про надання дозволу на зміну властивостей досліджуваного об'єкта – мобільного телефона «Alcatel». Експерт зазначив, що дослідження інформації, яка міститься в пам'яті мобільного телефона, передбачає безпосереднє його включення, що неодмінно призведе до внесення змін у файлову систему вказаного носія інформації. На підставі викладеного та керуючись ст.ст. 69, 242, 243, 244 КПК України, слідчий суддя задовольнив клопотання судового експерта[101].

У разі відхилення клопотання експерт має здійснити перегляд методів проведення експертизи. У разі неможливості проведення експертизи без використання руйнівних/частково руйнівних методів експерт повинен звернутись з повідомленням про неможливість проведення дослідження.

Перед підключенням носіїв інформації до тестового комп'ютера повинні бути забезпечені незмінність і збереження інформації. Так, наприклад, при підключенні досліджуваних накопичувачів на жорстких магнітних дисках до тестового комп'ютера для запобігання витоку важливої інформації з підключених накопичувачів на жорстких магнітних дисках має бути здійснено блокування можливості збереження даних на носіях, що підключаються до портів USB тестового комп'ютера. Блокування можливості

[101] Ухвала слідчого судді Жмеринського міськрайонного суду про задоволення клопотання від 03.04.2019 у справі № 130/82/19 (кримінальне провадження № 12019020130000019). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

збереження даних рекомендується здійснювати апаратними блокаторами, допускається блокування можливості збереження даних програмними засобами (засобами експертної операційної системи, спеціалізованим програмним забезпеченням).

Для встановлення придатності носіїв інформації для подальшого проведення дослідження рекомендується використання спеціалізованого програмного забезпечення. Наприклад, для накопичувачів на жорстких магнітних дисках можливо здійснення тестування на наявність збійних кластерів (ділянок на поверхні диска, що мають механічне або інше ушкодження). В якості однієї з програм, які можна застосувати для цього, може бути використана HDDScan. (HDDScan – це утиліта для тестування накопичувачів інформації (HDD, RAID, Flash)). Програма призначена для діагностики накопичувачів інформації на наявність BAD-блоків, перегляду S.M.A.R.T-атрибутів накопичувача, зміни спеціальних налаштувань (управління живленням, старт/стоп шпинделя, регулювання акустичного режиму).

Для відповіді на питання експертизи та визначення методів дослідження об'єкти підключаються до тестового комп'ютера експерта, на якому здійснюється підготовка робочих зон (директорій на тестовому комп'ютері експерта, містять усю досліджувану інформацію та інформацію, що має доказове значення у кримінальному провадженні). Результати попереднього дослідження і регламентована інформація про експерта, експертну установу, експертизу мають бути відображені у вступній і частково дослідницькій частинах висновку.

Виконується клонування/копіювання даних з наданих на експертизу носіїв інформації на робочу станцію експерта (тестовий комп'ютер). При проведенні аналізу даних, що містяться безпосередньо на самому носії, без їх попереднього копіювання на робочу станцію експерта, даний етап відсутній.

На робочій станції експерта створюється директорія, в якій будуть розміщені файли, що містять інформацію, необхідну для відповіді на поставлені запитання. У директорії розміщується інформація, отримана з об'єктів, наданих експертові, необхідна для проведення експертизи, але в своєму повному обсязі не є доказом у відповідному кримінальному провадженні. Таким чином, в даній

директорії можуть бути розміщені: повні образи носіїв інформації, log-файли, reg-файли, історія інтернет-активності, index-файли тощо. Така організація робочих зон вельми зручна при роботі з великою кількістю інформації, але не є обов'язковою.

При виборі експертом між дослідженням клонів/копій/образів і дослідженням інформації безпосередньо на носії потрібно керуватись тим, що у відповідності зі стандартами криміналістики експерти проводять дослідження або аналіз копій цифрових об'єктів – так виключається зміна або порушення цілісності даних оригіналів.

Дослідження безпосередньо самого носія можливе, якщо такий вид дослідження фізично не може внести зміни в інформацію (наприклад, через особливості носія – DVD-R) або у разі неможливості отримання копії, придатної для проведення дослідження (в цьому випадку необхідним є дозвіл особи, яка доручила проведення експертизи, на застосування частково руйнівних методів).

Копія вихідних цифрових даних для дослідження зазвичай називається образом[102]. Для того, щоб цей образ був юридичним еквівалентом оригіналу, він повинен являти собою абсолютну копію вихідних даних. Отже, кожен біт оригіналу повинен бути скопійований на образ.

Існують різні методи клонування носіїв інформації. Вибір того чи іншого методу обумовлюється конкретною ситуацією. Охарактеризуємо окремі з них.

Клонування з диска на диск у DOS – відносно швидкий спосіб дублювання даних. Цей спосіб клонування (drive-to-drive) відбувається повністю в операційній системі DOS, а досліджуваний накопичувач і накопичувач для збереження образу підключені до однієї і тієї ж системної плати. Перевагою вказаного методу є його простота, – потрібно тільки завантажувальний диск (наприклад, Acronis або EnCase) і накопичувач для збереження образу[103].

---

[102] Acronis TrueImage 7.0. URL: http://www.acronis.com/ru-ru/company/inpress/2004/09-04-ru-ixbt-trueimage-1-creating-image.html, свободный (дата звернення: 12.03.2021).

[103] Официальный экзамен EnCE: Сертифицированный пользователь EnCase. Учебное руководство. URL: http://computer-forensics-lab.org/pdf/encase_EnCE.pdf (дата звернення: 12.03.2021).

Іще одним способом клонування, який містить в собі переваги завантаження в DOS, є клонування даних по мережі. Цей спосіб дуже зручний для таємних операцій, коли необхідно швидко створити образ цільового накопичувача, поки його власник відсутній. Застосування даного методу може допомогти під час: клонування невидимих даних в області HPA або DCO; дублювання даних з накопичувача на жорстких магнітних дисках лептопа; швидкого клонування даних[104].

Результати попереднього дослідження і регламентована інформація про експерта, експертну установу, експертизу відображаються у вступній і частково дослідницькій частинах висновку.

На підготовчій стадії у вступній частині висновку вказуються: місце і час проведення експертизи; підстави проведення; інформацію про експертну установу, експерта; відмітка про попередження експерта про кримінальну відповідальність; питання, поставлені на експертизу; відмітка про редагування питання (у разі редагування формулювання питання експертом); інформація про об'єкти, які надійшли на дослідження; надані матеріали кримінального провадження, які відносяться до питань експертизи; інформація про заявлені клопотання, результати їх вирішення (може бути вказано/доповнено на наступних стадіях експертизи); відмітка про проведення повторної або додаткової експертизи; використана література (може бути вказана/доповнена на наступних стадіях експертизи).

У дослідницькій частині висновку зазначається інформація: про результати зовнішнього огляду об'єктів; про результати дослідження інформаційного простору носіїв інформації та їх придатність для проведення дослідження; про обрані методи дослідження носіїв інформації.

На нашу думку, дотримання окресленого алгоритму дій на підготовчій стадії СКТЕ сприятиме: 1) попередженню необґрунтованого застосування експертом частково руйнівних або руйнівних методів дослідження – внесення змін в інформацію, що міститься на досліджуваних об'єктах. У результаті чого під сумнів може бути поставлена не тільки придатність висновку як джерела доказів, а й самих об'єктів дослідження; 2) упущенню важливих артефактів,

[104] Официальный экзамен EnCE: Сертифицированный пользователь EnCase. Учебное руководство. URL: http://computer-forensics-lab.org/pdf/encase_EnCE.pdf (дата звернення: 12.03.2021).

неправильному трактуванню їх (експерт може дати неповний, недостовірний висновок); 3) отриманню самовідводу або відводу експерта через відсутність у нього необхідних знань (інформації про методи дослідження, умови їх застосування, експертний інструментарій та ін.); 4) скороченню термінів проведення СКТЕ; 5) зменшенню трудовитрат і вартості провадження експертизи; 6) унеможливленню приховування кримінального правопорушення.

Перейдемо до аналізу наступних складових алгоритму проведення СКТЕ.

На *аналітичній стадії* здійснюється ретельне дослідження об'єктів з використанням апаратно-програмних засобів – експертного інструментарію.

Аналітична стадія складається з двох етапів: попереднього, спрямованого на отримання загальної інформації про досліджувані об'єкти, і основного, на якому відбувається детальний аналіз з метою отримання інформації, що має значення для відповіді на питання, викладені у постанові (ухвалі).

В рамках попереднього етапу аналітичної стадії узагальнюється інформація про обсяг даних, їх структуру, налаштування, проводиться експрес-аналіз даних, файлів, формується уявлення про їх вигляд. Так для накопичувача на жорстких магнітних дисках на попередньому етапі будуть виконані такі дії (для інших об'єктів дослідження виконується за аналогією): 1) підрахунок хеш-сум; 2) перевірка фізичного розміру диска і порівняння його з розміром усіх областей дискового простору; 3) визначення і порівняння розмірів логічних розділів з розміром диска для визначення інформації про віддалені розділи або про невикористаний дисковий простір; 4) отримання інформації про налаштування тимчасових зон для кожного диска і застосування правильної зони, якщо це можливо; 5) перейменування розділів накопичувача на жорстких магнітних дисках так, як це необхідно («C», «D» і т. д.); 6) збір системної інформації: визначення типу оперативної системи, SP, дати установки оперативної системи; імені користувача та імені комп'ютера тощо; отримання інформації про профілі користувача (ім'я, SID, дата створення і останнього входу в систему); 7) експрес-аналіз даних: аналіз сигнатури файлів, перегляд перейменованих файлів; визначення зашифрованих файлів; визначення та монтування файлів-образів, контейнерів, архівів – VHD, VMDK, ZIP, RAR, Email-контейнери, Reg-файли та ін.; 8) аналіз включених, працюючих

сервісів; 9) здійснення сканування: пошук і аналіз вірусів; пошук і аналіз артефактів програм для стеганографії; 10) здійснення пошуку за ключовими словами: складання списку ключових слів; формування пошукового запиту, з використанням синтаксису обраного пошукового інструментарію; проведення пошуку – цільового (в певних директоріях), всього простору (включаючи нерозподілені області і видалені розділи); складання звіту за результатами пошуку; 11) фільтрація даних (на підставі метаданих – дата, час, розширення тощо).

В рамках основного етапу аналітичної стадії дослідження виконуються наступні дії: 1) аналіз файлів з використанням спеціалізованого програмного забезпечення; 2) аналіз основних областей (виконується для пошуку артефактів і / або іншої інформації); 3) аналіз системного реєстру (може допомогти в отриманні важливої інформації як про саму систему, як про додатки, так і про активність користувача; 4) аналіз артефактів оперативної системи, які можуть містити важливу інформацію для відповіді на питання експертизи (наприклад, резервних копій, файлів Event Logs (.evt, .evtx); Shell bags; Jump Lists; LNK-файлів та ін.; 5) аналіз слідів роботи програмного забезпечення. Визначення наявності програмного забезпечення (наприклад, Wiping tools, P2P, Sticky Notes, програмне забезпечення для злому та ін.), аналіз журналів (логів), налаштувань, реєстру тощо; 6) здійснити аналіз тимчасової інформації, що міститься в пам'яті (по можливості); 7) аналіз листування (e-mail, соц. мережі) (пошук встановлених поштових клієнтів, архівів повідомлень поштових клієнтів, перегляд встановленого програмного забезпечення обміну миттєвими повідомленнями (QIP, ICQ та ін.), архівів повідомлень; аналіз інтернет-активності користувача (Facebook, Twitter та ін.)); 8) аналіз інтернет-активності (визначити встановлені браузери і здійснити для них аналіз артефактів (файлів історії відвідування, тимчасових директорій, куків (cookies), кеша сторінок, обраного, закладок, панелі інструментів, плагінів, системного реєстру, віддаленої інформації)[105].

[105] Смолина А. Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дисс. … канд. техн. наук : 05.13.19 «Методы и системы защиты информации, информационная безопасность». Томский государственный университет систем управления и радиоэлектроники. Томск, 2017. С. 66–68.

Хід проведення дослідження, використані методи фіксуються. На завершення аналітичної стадії експертом даються попередні висновки, які уточняються на наступних стадіях дослідження.

Інформація про уразливість процесів переробки інформації в інформаційних системах (важлива при розслідуванні кримінальних правопорушень, пов'язаних з порушенням інформаційної безпеки у відкритих комп'ютерних мережах, розкраданням (руйнуванням, модифікацією) інформації і порушенням інформаційної безпеки) формується саме на аналітичній стадії. Відповідно до правил проведення СКТЕ експерти в своєму висновку відповідають на питання експертизи та не дають рекомендацій щодо вдосконалення існуючих засобів захисту інформації та забезпечення інформаційної безпеки. Якщо ж це (рекомендації щодо вдосконалення існуючих засобів захисту інформації та забезпечення інформаційної безпеки) є питанням експертизи, то дані рекомендації даються в результаті її узагальнення на синтезуючій стадії.

Інформація, отримана на аналітичної стадії, викладається в тексті висновку СКТЕ і може бути використана фахівцями з інформаційної безпеки для вдосконалення існуючих засобів захисту інформації та забезпечення інформаційної безпеки[106].

Експеримент. Наявність стадії експерименту залежить від кожної конкретної ситуації, його форма базується на завданнях і цілях експертного дослідження. Метою проведення експертного експерименту є виявлення механізму взаємодії об'єктів експертного дослідження і (або) механізму слідоутворення, його окремих параметрів.

В ході експертного експерименту експерт вивчає питання, процеси та умови, які його цікавлять. Експеримент може бути проведений як в експертній установі, так і поза ним, та включає в себе такі етапи: проектування; підготовку; проведення; підбиття підсумків.

У дослідницькій частині висновку експерт повинен детально описати умови проведення експерименту і його результати. Резуль-

[106] Смолина А. Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дисс. … канд. техн. наук : 05.13.19 «Методы и системы защиты информации, информационная безопасность». Томский государственный университет систем управления и радиоэлектроники. Томск, 2017. С. 68.

тати експерименту оформляються у вигляді попередніх висновків у даному кримінальному провадженні[107].

Синтезуюча стадія проведення СКТЕ є свого роду узагальненням інформації, отриманої на попередніх стадіях експертизи. Залежно від конкретних завдань, вирішення яких необхідне для відповіді на поставлені запитання, розглядаються відповідні артефакти.

До основних завдань (діагностичних, ідентифікаційних, класифікаційних) і артефактів, що розглядаються для їх вирішення в операційних системах сімейства Windows слід віднести: визначення інформації про файли (завдання пошуку файлів), у т. ч. віддалені; визначення інформації про відкриття / створення файлу; визначення інформації про завантаження файлу; визначення інформації про запуск програм; визначення використання / підключення USB-пристроїв; визначення фізичного знаходження (локалізації) користувача; визначення інформації про обліковий запис; визначення Інтернет-активності користувача.

Для інших оперативних систем сімейства Windows артефакти будуть відрізнятися їх розташуванням (адресою директорій і назвою файлу), а для деяких завдань і складом. Детальна інформацію про склад і розташування артефактів можна віднайти на офіційному сайті компанії-розробника операційної системи[108].

Під час *результативної стадії* відбувається підведення підсумків, оцінюються результати проведених досліджень, здійснюється остаточне оформлення дослідницької (і, якщо потрібно, вступної) частини висновку.

Результатом заключної стадії є формулювання та оформлення висновків в розділі висновку «Висновки». У ньому повинні бути обов'язково відображені всі питання експертизи та відповіді на них. Висновок по кожному питанню повинен бути розгорнутим, бажано із посиланням на інформацію в дослідницькій частині висновку, виходячи з якої зроблені висновки.

---

[107] Смолина А. Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дисс. … канд. техн. наук : 05.13.19 «Методы и системы защиты информации, информационная безопасность». Томский государственный университет систем управления и радиоэлектроники. Томск, 2017. С. 70.

[108] Там само. С. 72.

За результатами проведення СКТЕ у висновку експерта повинно бути зазначено: 1) коли, де, ким (ім'я, освіта, спеціальність, свідоцтво про присвоєння кваліфікації судового експерта, стаж експертної роботи, науковий ступінь, вчене звання, посада експерта) та на якій підставі була проведена експертиза;2) місце і час проведення експертизи; 3) хто був присутній при проведенні експертизи; 4) перелік питань, що були поставлені експертові; 5) опис отриманих експертом матеріалів та які матеріали були використані експертом; 6) докладний опис проведених досліджень, у тому числі методи, застосовані у дослідженні, отримані результати та їх експертна оцінка; 7) обґрунтовані відповіді на кожне поставлене питання (ч. 1 ст. 102 КПК України)[109].

Також у висновку експерта обов'язково повинно бути зазначено, що його попереджено про відповідальність за завідомо неправдивий висновок та відмову без поважних причин від виконання покладених на нього обов'язків. Якщо при проведенні експертизи будуть виявлені відомості, які мають значення для кримінального провадження і з приводу яких не ставилися питання, експерт має право зазначити про них у своєму висновку. Висновок підписується експертом (ч. ч. 2, 3 ст. 102 КПК України)[110].

Типовими недоліками щодо оформлення результатів дослідження у висновках експертів є: недотримання норм процесуального законодавства (ст. ст. 69, 101, 102 КПК України); порушення логічних законів вивідного знання; недотримання загальних методичних рекомендацій з дослідження об'єктів експертизи; відсутність опису стандартів, методик, програмних продуктів та вимірювального обладнання, які були використані під час проведення досліджень[111].

Використання у висновках експертів наукової або квазінаукової мови, посилань на наукові підходи, авторські методики, наведення в них реальних та вигаданих регалій експерта, у зв'язку

[109] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

[110] Там само.

[111] Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : дис. … канд. юрид. наук : 12.00.09. Х., 2017. С. 13.

з відсутністю у правозастосовувача спеціальних знань, сприяє «психологічному тиску» на нього, за якого доказова сила експертизи необґрунтовано суб'єктивно підвищується. Даний аспект може використовуватися з метою маніпулювання думкою суду, штучним розширенням доказової бази за кримінальним провадженням сторонами процесу[112].

В теорії судової експертології і в нормативних актах, які регулюють форму і зміст висновку експерта, постійно підкреслюється, що хоча експерт при описі дослідження користується науковою термінологією, науковим стилем мови, але адресатом експертного висновку є особи, які не володіють спеціальними знаннями (слідчий, прокурор, суддя, інші учасники процесу).

Тому мова експерта повинна бути по можливості простою і зрозумілою, наведені у висновку формули необхідно роз'яснювати і коментувати[113].

У разі необхідності експертом подаються клопотання (клопотання можуть бути заявлені на будь-якій стадії дослідження) про: ознайомлення з матеріалами кримінального провадження, що стосуються предмета експертизи; надання додаткових матеріалів, що мають відношення до експертизи; залучення іншого експерта, спеціаліста; участь у процесуальних діях; застосування руйнуючих / частково руйнуючих методів. Інформація про подані клопотання і їх вирішення відображається у висновку.

Слід зазначити, що при проведенні СКТЕ експерт має право відмовитися від дачі висновку в разі виявлення на будь-якій стадії дослідження таких обставин: 1) експерт не володіє достатньою компетентністю для вирішення поставлених завдань; 2) в експертній установі відсутня матеріально-технічна база, необхідна для проведення дослідження; 3) недостатньо даних після заявлених клопотань; 4) немає даних науки для вирішення поставлених питань. У разі відмови від дачі висновку із вказаних причин експер-

[112] Проблемы проведения и научного обеспечения судебных экспертиз. URL: https://ceur.ru/library/articles/ pravo/item127028.

[113] Россинская Е. Н. Гносеологические и деятельностные экспертные ошибки при использовании в производстве судебных экспертиз современных технологий. *Вестник Московского университета МВД России*. 2015. № 3. С. 20.

том оформляється повідомлення про неможливість проведення дослідження[114].

Описана методика проведення СКТЕ, яка містить рекомендації щодо алгоритму її проведення, застосування окремих інструментальних методів, вимоги щодо оформлення висновку експерта, його структури та результатів, є загальною, уніфікованою, може бути придатною для вирішення широкого кола окремих ідентифікаційних, діагностичних і класифікаційних завдань. Тобто, може бути спрямована на вирішення запитань, що стосуються комп'ютерної інформації, програмних засобів, обчислювальних мереж і їх елементів, апаратних засобів. Водночас, слід зазначити, що у разі використання такої методики в якості приватної, вона має певні обмеження, пов'язані з описом окремих методів, які можна застосувати для певного кола об'єктів. Основне обмеження пов'язане із можливістю використання деяких методів для певних операційних систем (Windows).

Описаний підхід до визначення послідовності методів проведення СКТЕ, на нашу думку, матиме позитивний ефект, а саме: скорочення термінів проведення експертизи; зменшення часу на розробку окремої методики СКТЕ; мінімізація витрат на проведення експертизи.

[114] Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

6 ТИПОВІ ПОМИЛКИ ПРИ ПРОВЕДЕННІ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Висновок експерта повинен ґрунтуватися на наукових, технічних або інших спеціальних знаннях експерта, на відомостях, які експерт сприймав безпосередньо або вони стали йому відомі під час дослідження матеріалів, що були надані для проведення дослідження. Експерт дає висновок від свого імені і несе за нього особисту відповідальність (ч.ч. 2, 3 ст. 101 КПК України).

Однак, як і будь-якій людині, судовому експерту можуть бути властиві помилки, прорахунки, упущення. У той же час, помилки, допущені експертом в процесі проведення експертизи і підготовки висновку за її результатами, можуть зробити цей доказ нікчемним[115]. Об'єктивізація процесу доказування вимагає попередження і своєчасного розпізнавання експертних помилок, а, в результаті, – викорінення причин, що їх породжують.

Помилки експерта слід відрізняти від його кримінально протиправних дій. Так, за надання завідомо неправдивого висновку, за відмову без поважних причин від виконання покладених на нього обов'язків, а також за розголошення даних, що стали йому відомі під час проведення експертизи, експерт несе кримінальну відповідальність згідно зі ст. 365 КК України.

Численні проблеми виникають не лише під час виявлення, фіксації, вилучення (пакування) електронної інформації, її носіїв, а й безпосередньо під час проведення СКТЕ. Причини таких помилок можуть бути об'єктивними і суб'єктивними. До типових експертних помилок, які мають об'єктивну природу, слід віднести: недосконаліть, відсутність розробленої та апробованої експертної мето-

[115] Предупреждение экспертных ошибок / под ред. Д. Я. Мирского, В. Ф. Статкуса, А. К. Педенчука. М., 1990. С. 25.

дики; застосування методів і приладів, які перебувають у стадії експериментальної розробки, не мають достатньої чутливості або роздільної здатності; застосування несправного або несертифікованого обладнання; використання неадекватних математичних моделей і комп'ютерних програм, неліцензійного програмного забезпечення; відсутність повних даних, що характеризують ідентифікаційну та діагностичну значимість ознак, стійкість їх відображень у слідах та ін.[116].

До суб'єктивних причин експертних помилок відноситься, насамперед, професійна некомпетентність експерта: незнання сучасних експертних методик; неповнота дослідження, його однобічність; невміння застосовувати сучасні експертні технології; відсутність навичок роботи з апаратурою, технічними, комп'ютерними засобами та системами; неправильна оцінка ідентифікаційної значущості ознак тощо. Помилками слід визнати й професійні упущення експерта (недбалість, неакуратність, неуважність, поверхневе проведення дослідження), які можуть бути пов'язані з певними рисами особистості експерта, як-то: дефекти або недостатня гострота органів зору експерта; хвороба, перевтома, стрес, емоційне або психічне напруження, поспіх; невпевненість у своїх знаннях; підвищена сугестивність; недовірливість; конформізм, або навпаки зайва самовпевненість, амбітність, нехтування думкою колег тощо[117].

Причина помилковості висновку експерта може бути не тільки в допущених експертом помилках. Вони часто стають наслідком слідчих і судових помилок, пов'язаних з призначенням судової експертизи і оцінкою її результатів. Експертне дослідження може бути виконано бездоганно, зроблені висновки повністю відповідають отриманим результатам. Але якщо вихідні дані були помилковими або досліджувані об'єкти не мали відношення до кримінального провадження, були фальсифіковані, то й висновок експерта в аспекті встановлення обставин кримінального правопорушення

[116] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи. Судебная экспертиза. М. : Проспект, 2010. С. 214; Виницкий Л. В., Мельник С. Л. Экспертная инициатива в уголовном судопроизводстве. М. : Экзамен, 2009. С. 118.

[117] Зинин А. М. Теория судебной экспертизы : учебник для вузов / под ред. Е. Р. Россинской. М., 2013. С. 19.

виявиться помилковим. Однак у цьому випадку не можна говорити про помилку експерта, оскільки причиною помилкового висновку є помилка суб'єкта, який призначив експертизу, або його навмисні неправильні дії, правопорушення.

За своєю природою експертні помилки неоднорідні і можуть бути розділені на три класи: помилки процесуального характеру; гносеологічні помилки; діяльнісні (операційні) помилки[118].

Помилки експерта процесуального характеру полягають у порушенні експертом процесуального режиму і процедури проведення експертизи: вихід експерта за межі своєї компетенції; вираження експертної ініціативи в непередбачених законом формах; обґрунтування висновків матеріалами справи, а не результатами дослідження; самостійне збирання матеріалів та об'єктів експертизи; здійснення несанкціонованих судом (слідчим) контактів із зацікавленими особами, прийняття доручення на проведення експертизи і матеріалів від неуповноважених осіб; недотримання через незнання процесуальних вимог до висновку експерта (в тому числі відсутність у висновку необхідних за законом реквізитів; обґрунтування висновків не результатами дослідження, а матеріалами справи та ін.)[119].

Аналіз наукової та методичної літератури дозволив визначити такі типові помилки процесуального характеру при проведенні СКТЕ: порушення процедури попередження експерта про кримінальну відповідальність за дачу завідомо неправдивого висновку; відсутність відомостей про експертів, які виконували експертизу: їх освіта; експертна спеціальність, стаж експертної роботи тощо; відсутність дослідницької частини висновку як такої; відсутність у висновку докладного опису об'єктів, представлених на експертизу; відсутність докладного опису технології експертного дослідження, що включає рекомендовану (сертифіковану) експертну методику, а якщо такої немає посилань на наукову літературу, яка містить рекомендації з дослідження таких об'єктів; відсутність

---

[118] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма, 2001. С. 187.

[119] Россинская Е. Р. Ошибки судебной экспертизы: классификация, выявление, предупреждение. *Союз криминалистов и криминологов*. 2014. № 2. С. 134.

опису здійснених експертних експериментів і умов їх проведення; відсутність висновків експерта і його власноручного підпису; підпис експертом частин висновку, які виконані без його участі іншими експертами тощо.

Науковцями також вказується на існування у діяльності експертів діяльнісних (операційних), гносеологічних, логічних, фактичних (предметних) помилок. Надзвичайно важко провести чітку грань між ними, адже одні помилки можуть бути причиною, наслідком інших, їх частиною, переплітатись з ними тощо. Так чи інакше, допущення помилок при проведенні експертизи може мати вирішальне значення у кримінальному провадженні. Говорячи про помилки, що виникають при проведенні СКТЕ, особливу увагу приділимо типовим експертним помилкам та їх причинам з метою вироблення науково-обґрунтованих рекомендацій щодо їх недопущення, виявлення, виправлення та попередження.

Насамперед зазначимо, що важливим при проведенні СКТЕ є додержання принципів збереження цифрових даних. Міжнародною організацією з комп'ютерних доказів (IOCE) вироблено основні принципи, якими слід керуватися при пошуку, виявленні, фіксації, вилучення, дослідження та зберіганні цифрових доказів: при роботі з цифровим доказом повинні бути дотримані всі загальні судово-експертні та процесуальні положення; при вилученні цифрових доказів вироблені дії не повинні змінювати цифровий доказ; якщо особі необхідно отримати доступ до оригінального цифрового доказу, особа повинна мати відповідну підготовку; уся діяльність з вилучення, доступу, зберігання або передачі цифрових доказів повинна бути повністю задокументована, захищена і доступна для аналізу; особа несе відповідальність за те, що буде дбайливо виконувати всі дії з цифровим доказом, поки цифровий доказ знаходиться в його розпорядженні; будь-яка організація, що відповідає за вилучення, доступ, зберігання або передачу цифрових доказів відповідає за відповідність даним принципам[120].

[120] Guidelines for Best Practices in Examination of Digital Evidence. Checklist for handling digital Image and Audio evidence (Инструкция по обращению с цифровыми изображениями и аудиодоказательствами) IOCE, December 2000. Http:// ioce.org/ fileadmin/ user_upload/ 2000/ ioce %202000 %20digital %20image %20audio_checklist %20for %20handling %20digital %20evid.doc (дата звернення: 12.03.2021).

На жаль, експерти не завжди дотримуються цих принципів і положень, допускаючи порушення експертної методики СКТЕ. Так, відповідно до методичних рекомендацій і принципів дослідження цифрових доказів категорично забороняється здійснювати завантаження з досліджуваного носія інформації (жорсткого диска). При завантаженні комп'ютера може бути змінена інформація, що зберігається в файлах-протоколах його роботи. Для нормальної роботи операційної системи після встановлення жорсткого диска в інший комп'ютер може знадобитися установка драйверів пристроїв, оскільки конфігурація комп'ютера може бути змінена. Подекуди експерт у висновку не зазначає, чи провадив він встановлення будь-яких драйверів для забезпечення роботи системного блоку. Тим часом при дослідженні висновку експерта встановлюється наявність піктограми в правому нижньому кутку екрану, що свідчить про підключення до комп'ютера USB-накопичувача (флеш-пам'яті, картрідера або переносного жорсткого диска), та супроводжується автоматичною установкою драйверів пристрою для забезпечення його роботи, при цьому початковий стан жорсткого диска і його зміст змінюються[121].

Слід також зазначити, що експертним шляхом не може бути вирішене питання про правовласників, які є однією зі сторін процесу (цивільним позивачем, цивільним відповідачем, потерпілим), а встановлення автентичності прав не входить у компетенцію експерта. Експерт може лише визначити характеристики програмних, апаратних та інформаційних продуктів, представлених на експертизу в якості об'єкта дослідження, і вказати на ознаки, які вказують на контрафактність[122]. Іншими словами, факт порушення авторських прав є елементом складу злочину, а тому повинен бути встановлений слідчим, а не експертним шляхом.

Аналогічно й можливість правозастосовнику кваліфікувати програму для комп'ютерного носія як шкідливу, залежить від рішення уповноваженої особи. Частка експерта у встановленні зазна-

[121] Сабадаш Р. В. Судова комп'ютерно-технічна експертиза: правові підстави й особливості призначення. *Науковий вісник Чернівецького університету*. 2013. Вип. 660. С. 135.

[122] Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юрид. мир, 2007. С. 17.

ченого факту лежить лише в обґрунтованому виявленні ним таких ознак, які в подальшому сприятимуть слідчому, прокуророві, суду у прийнятті остаточного рішення у кримінальному провадженні. В експертній практиці нерідкі випадки, коли експерти виходять за межі своєї компетенції, самі того не підозрюючи. Наприклад, визначення вартості програмних продуктів, наданих на дослідження, і визначення шкоди, завданої правовласнику.

Таким чином, визначення розміру шкоди, контрафактності творів і встановлення правовласника не входять до компетенції експерта в галузі СКТЕ.

Необхідно уточнити, що окремі із вказаних помилок експерта мають методичний характер, та потребують детального дослідження.

Основним принципом при проведенні судових експертиз, і зокрема СКТЕ, є принцип незмінності речових доказів, суть якого полягає у тому, що інформація на представленому на дослідження носії даних не повинна бути змінена. Дотримання цього принципу можливе при використанні спеціальних апаратних блокіраторів (Tableau, Fast Block), програмного забезпечення, що блокує запис, по порту, до якого підключений досліджуваний об'єкт, створення точного побітового способу представленого об'єкта і його подальше дослідження. Недотримання цього принципу може призвести до фатальних зміни на рівні даних (затирання криміналістично значимої інформації, представленої в неявному вигляді).

Досить поширеною помилкою експерта є неповнота проведення дослідження, пов'язана з упущенням експертом об'єктів, які є складовою частиною єдиного інформаційного процесу. Найбільш часто це зустрічається в тих випадках, коли експертне дослідження стосується не одиничного об'єкта, а системи взаємопов'язаних об'єктів, що включають в себе апаратне, програмне та інформаційне забезпечення.

Яскравим прикладом цього є дослідження сервера провайдера і кінцевого обладнання користувача (комп'ютера) в разі встановлення можливості здійснення доступу користувачем до певних Інтернет-ресурсів в певний час. На жаль, при цьому з поля зору експерта випадає одна важлива складова, яка несе криміналістично значиму інформацію, а саме – проміжне обладнання. Зазвичай під

час аналізу даних, наданих провайдером, встановлюються IP-адреси роутера, а не користувача. Найчастіше це обумовлено тим, що у великих провайдерів найчастіше не ведеться облік дій кінцевих користувачів, а ведеться тільки облік звернень, що йдуть від загальних роутерів, до яких можливе підключення від 5 до 100 кінцевих користувачів. У зв'язку з цим серйозною помилкою експерта буде виключення з дослідження інформації, що міститься в роутері, проміжну ланку між провайдером і кінцевим користувачем. Така ситуація, пов'язана з виключенням частини системи, може зустрічатися при проведенні дослідження, пов'язаного з аналізом великих взаємопов'язаних об'єктів[123].

До типових помилок експерта при проведенні СКТЕ слід віднести випадки, коли експерт не здійснює ретельний зовнішній огляд об'єкта дослідження або переносить цю стадію проведення дослідження на наступні етапи експертизи, і приступає, наприклад, до перевірки працездатності об'єкта. Це неприпустимо, адже здійснення зовнішнього огляду допомагає експерту визначити стан наданого об'єкта, виявити його недоліки і зовнішні дефекти, комплектність, а отже, дає можливість визначитися з алгоритмом проведення всього експертного дослідження, застосованими методиками і використовуваним обладнанням. Такі дії допоможуть у подальшому уникнути помилок при безпосередньому проведенні експертного дослідження. У таких випадках залишається невідомим, в результаті чого були отримані механічні пошкодження об'єкта дослідження, чи були вони в момент надходження об'єкта на дослідження або стали результатом помилки експерта[124].

При проведенні дослідження і виявлення програм, які визначаються антивірусними засобами як шкідливі, експертами допускаються й інші помилки. Так, очевидно, що речові докази, зазвичай, повинні повертатися замовнику в тому вигляді, в якому вони надійшли на дослідження. У тих випадках, коли експерт виявив шкідливу програму, він зобов'язаний зазначити в дослідницькій частині висновку, що ця шкідлива програма залишилася на машин-

[123] Сабадаш Р. В. Судова комп'ютерно-технічна експертиза: правові підстави й особливості призначення. *Науковий вісник Чернівецького університету*. 2013. Вип. 660. С. 136.

[124] Там само. С. 137.

ному носії без зміни. Таке повідомлення є обов'язковим через небезпеку подальшого необережного поширення вірусу. Однак здебільшого це не робиться. Навпаки, в окремих випадках експерти повідомляють, що в надісланій на дослідження програмі був виявлений вірус і знищений, хоча дозвіл на здійснення такої операції експерт не отримав.

Діяльнісні (операційні) помилки пов'язані зі здійснюваними експертом операціями (процедурами) і можуть полягати у: а) порушенні запропонованої послідовності цих процедур; б) неправильному використанні засобів дослідження або використання непридатних засобів, наприклад використання апаратури, яка давно не проходила перевірку; в) отриманні неякісного порівняльного матеріалу тощо. У багатьох випадках фактичні помилки супроводжуються діяльнісними, і навпаки діяльнісні – фактичними, оскільки і ті й інші пов'язані з професійною компетенцією експерта і можуть бути виявлені, як правило тільки особами, що володіють відповідними спеціальними знаннями. Тому доцільно розглядати ці помилки у комплексі за стадіями експертного дослідження.

Найбільш поширені помилки на підготовчій стадії СКТЕ: непридатність об'єктів для дослідження; невірне уявлення про об'єкти дослідження; недостатня кількість або низька якість порівняльних зразків; помилкові експертні версії, які згодом не були уточнені; вибір методів або методик дослідження, які не відповідають об'єктам.

Діяльнісні (операційні) помилки можуть мати як об'єктивні причини (використання приладів та інструментів, несправних або котрі мають достатньою точністю, роздільною здатністю; використання неадекватних математичних моделей і комп'ютерних програм), так і суб'єктивні (дефекти органів сприйняття експерта і його неординарні психічні стани (стрес, конфлікт в колективі, втома тощо))[125]. Виявлення таких помилок можливе, головним чином, при повторному дослідженні, а в попередженні їх відіграє роль постійний контроль за справністю приладів для проведення дослідження. Професіоналізм судового експерта визначається

[125] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма, 2001. С. 188.

також і його здатністю враховувати фактори, що впливають на результати дослідження, умінням визначати достовірність зроблених висновків та ін.

На переконання Р. С. Бєлкіна, гносеологічні помилки кореняться в складнощах процесу експертного пізнання. Вони можуть бути допущені при пізнанні сутності, властивостей, ознак об'єктів експертизи, відносин між ними, а також при оцінці результатів пізнання, підсумків експертного дослідження, їх інтерпретації. Вони поділяються на логічні і фактичні (предметні)[126].

Логічні помилки пов'язані з порушенням в акті мислення законів і правил логіки, некоректним застосуванням логічних прийомів і операцій, наприклад змішання причинного зв'язку з простою послідовністю в часі або обґрунтування тези аргументами, з яких дана теза логічно не випливає. Такі помилки зазвичай пов'язані з різними логічними операціями і видами умовиводів. Так, можна виділити помилки в розподілі понять, у визначенні понять, помилки в індуктивному висновку, помилки в дедуктивних умовиводах, помилки в доказі: по відношенню до тези, до аргументу, до демонстрації[127].

У висновках експертів за результатами СКТЕ нами виявлено й інші логічні помилки: висновки експерта недостатньо мотивовані; по одному і тому ж предмету дані суперечливі висновки експертів; відсутня логічна обумовленість послідовності стадій експертного дослідження; висновок не є логічним наслідком здійсненого експертом дослідження; невідповідність висновків і дослідницької частини висновку; дослідницька частина формулюється в ймовірній формі, а висновки – в категоричній, що з дослідження не випливає або відповідь на питання наведено тільки у висновках, а в дослідній частині обґрунтування цієї відповіді взагалі відсутня.

Фактичні (предметні) помилки виникають від спотвореного уявлення про відносини між предметами об'єктивної дійсності, можуть бути помічені і виправлені тільки тим, хто знайомий з самим предметом, про який йде мова. На практиці мають місце

---

[126] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма, 2001. С. 187.

[127] Ивин А. А., Никифоров А. Л. Словарь по логике. М., 1997. С. 261.

випадки використання для обґрунтування експертного висновку виявлених при дослідженні одного об'єкта-носія експертами різних спеціальностей (або одним експертом, який володіє спеціальними знаннями з різних спеціальностей) ознак, які не можуть утворювати сукупність, але повинні аналізуватися окремо для кожного виду (роду) експертиз.

На завершальній стадії проведення СКТЕ при формулюванні висновків також можуть бути допущені фактичні та операційні помилки. До таких помилок відноситься відсутність синтезуючої частини у висновку комісійної або комплексної експертизи. При проведенні комплексних експертиз неправильна інтерпретація одними членами комісії експертів ознак або проміжних висновків, виявлених іншими експертами. Нерідко експерти змішують категоричний висновок про родову (групову) належність з імовірним виведенням. Більш того, висновок у ймовірній формі дається умоглядно, без будь-якого обґрунтування, хоча аналогічно до категоричного судження, такий висновок повинен ґрунтуватися на достатній сукупності достовірно встановлених проміжних даних і високого ступеня ймовірності їх існування. В іншому випадку слід відмовитися від вирішення питання. Хоча використання таких висновків правозастосовником і обмежено, однак вони не повинні бути голослівними, оскільки можуть сприяти висуненню і перевірці версій, встановленню існування фактів тощо.

Експертні помилки при проведенні СКТЕ можуть бути виявлені: при перевірці самим експертом ходу і результатів проведеного ним дослідження на будь-якій його стадії, і особливо на стадії формування висновку; під час аналізу експертом або спеціалістом висновків попередніх експертиз; керівником експертної установи у ході контрольної діяльності; слідчим, у провадженні якого знаходиться справа; в ході аналізу і обговорення результатів експертного дослідження, здійснюваного комісією експертів при проведенні однорідної комісійної і комплексної експертизи; під час оцінки висновку експерта судом відповідної інстанції; в процесі узагальнення експертної практики, що здійснюється з практичною або науковою метою.

Істотне для кримінального провадження значення має виявлення тих помилок, які призвели або могли спричинити неправиль-

ний висновок експерта. При виявленні таких помилок експерт або керівник експертної установи зобов'язаний довести до відома особу, орган, який призначив експертизу. Експерт (експерти) повинен вжити заходів до недопущення такої помилки у своєму дослідженні. Часто експертні помилки виявляються при оцінці висновку судом (слідчим)[128].

Якщо помилка не впливає на висновок експерта, вона може бути нейтралізована або усунена шляхом його допиту або призначення додаткової експертизи. Приміром, з метою роз`яснення висновку експерта слідчий суддя Вищого антикорупційного суду у справі № 760/24486/19 за відсутності підстав для проведення додаткового чи повторного дослідження здійснив допит експерта, який проводив дослідження жорсткого диску. Експерт повідомив, що під час досудового розслідування комп`ютер не вилучався і речовим доказом не визнавався, що позбавляє можливості призначати експертизу в частині дослідження цього комп`ютера[129].

Якщо висновок експерта буде визнано неповним або неясним, судом може бути призначена додаткова експертиза, яка доручається тому самому або іншому експерту (експертам) (ч. 1 ст. 113 КК України)[130]. В іншому випадку може бути призначена повторна експертиза. Зокрема, коли є сумніви у правильності висновку експерта, пов`язані з його недостатньою обґрунтованістю чи з тим, що він суперечить іншим матеріалам кримінального провадження, а також за наявності істотного порушення процесуальних норм, які регламентують порядок призначення і проведення експертизи. Істотними можуть визнаватися, зокрема, порушення, які призвели до обмеження прав обвинуваченого чи інших осіб.

---

[128] Россинская Е. Р. Ошибки судебной экспертизы: классификация, выявление, предупреждение. *Союз криминалистов и криминологов*. 2014. № 2. С. 134.

[129] Ухвала слідчого судді Вищого антикорупційного суду про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 30.09.2019 у справі №760/24486/19 (кримінальне провадження № 42018000000002019). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

[130] Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.03.2021).

Показовим у даному випадку є рішення слідчого судді Вищого антикорупційного суду у справі № 760/24486/19, у якій адвокат ні в клопотанні, ні в судовому засіданні не зазначив яку саме експертизу в кримінальному провадженні просить провести, враховуючи те, що первинна комп`ютерно-технічна експертиза вже проведена, а неясності висновку шляхом допиту експерта роз`яснені. Підстав для проведення додаткової чи повторної експертизи адвокатом наведено не було. Крім того, як вбачається з переліку поставлених на вирішення експерта запитань, вони повністю дублюються із тими, пояснення на які надані експертом, який проводив первісну експертизу, під час допиту детективом. З огляду на викладене, слідчий суддя дійшов висновку, що захисником в клопотанні та в судовому засіданні не наведено достатніх відомостей, що вказують на можливість досягнення мети у разі призначення комп'ютерно-технічної експертизи експертизи, тому підстави для задоволення клопотання відсутні[131].

Таким чином, в основі усіх видів експертних помилок при проведенні СКТЕ так чи інакше лежить недостатня компетентність особи, яка ініціювала проведення експертизи, або судового експерта. В світлі використання сучасних технологій при проведенні даного виду експертизи визначальне значення у запобіганні експертним помилкам має підвищення компетентності експертів, постійне вивчення нових методів і досягнень у сфері наукового знання.

[131] Ухвала слідчого судді Вищого антикорупційного суду про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 30.09.2019 у справі №760/24486/19 (кримінальне провадження № 42018000000002019). URL: https://conp.com.ua/search/lawsuit (дата звернення 12.03.2021).

7 ОЦІНКА ВИСНОВКУ ЕКСПЕРТА У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, В ЯКИХ БУЛО ПРИЗНАЧЕНО СУДОВУ КОМП'ЮТЕРНО-ТЕХНІЧНУ ЕКСПЕРТИЗУ

Уповноважені учасники кримінального процесу – слідчий, прокурор, слідчий суддя, суд здійснюють аналіз доказів з позиції об'єктивного критика, котрий перевіряє відповідність його положень законодавчо закріпленим процесуальним вимогам. Певну специфіку має оцінка висновку експерта як джерела доказів, під якою зазвичай розуміють встановлення належності, допустимості та достовірності висновку. Така оцінка здійснюється під час досудового розслідування та під час судового розгляду.

Через зростання складності висновків експерта в зв'язку із застосуванням високотехнологічних методів, засобів дослідження і обладнання, з виникненням нових родів та видів судових експертиз[132] зі складним ілюстративним матеріалом у вигляді діаграм, таблиць, креслень, схем ускладнилися й завдання оцінки висновку. Яскравим прикладом у цьому плані є висновок експерта за результатами проведення судової комп'ютерно-технічної експертизи.

Оцінка висновку експерта здійснюється суб'єктами доказування за загальними правилами, встановленими ст. 94 КПК України, з урахуванням специфіки цього джерела доказів, зумовленої його правовою природою, особливостями його змісту та процесуальної форми, специфікою отримання під час кримінального провадження[133].

---

[132] Шутемова Т. В. Оценка прокурором заключения судебного эксперта по уголовным делам. *Вестник Волжского университета имени В. Н. Татищева*. 2018. № 3. Т. 1. С. 193.

[133] Воробчак А. Р. Висновок експерта як джерело доказів у кримінальному провадженні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.09; Нац. ун-т «Одес. юрид. акад.». Одеса, 2019. С. 12.

Слідчий, прокурор, слідчий суддя, суд наділені як процесуальними, так і непроцесуальними можливостями для перевірки та оцінки висновку експерта. У зв'язку з цим важливим елементом є дослідження своєрідних підходів і видів оцінки висновку експерта при розслідуванні кримінальних правопорушень, у яких було проведено СКТЕ[134].

За змістом ч. 2 ст. 9 КПК, на стадії досудового розслідування прокурор, керівник органу досудового розслідування, слідчий зобов'язаний дослідити обставини кримінального провадження та надати обставинам належну правову оцінку, забезпечити прийняття законних і неупереджених процесуальних рішень. Вони, а також слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення (ч. 1 ст. 94 КПК)[135].

Тобто для того, щоб стверджувати про те, що обставинам кримінального провадження надана належна, а не спотворена правова оцінка, слідчий, прокурор повинні покроково виконати наступні дії, та продемонструвати те, що: зібрані ними матеріали є доказами (ч. 1 ст. 84 КПК) (містять фактичні (беззаперечні), а не будь-які данні, отримані в передбаченому КПК порядку, мають значення для цього кримінального провадження); отримані з передбачених процесуальних джерел (ч. 2 ст. 84 КПК); кожен з цих доказів перевірений та оцінений з точки зору належності, допустимості, достовірності; сукупність зібраних доказів оцінена з точки зору достатності та взаємозв'язку; оцінка доказів зроблена не як заманеться, а керуючись законом (з посиланням на цей закон); внутрішнє переконання слідчого, прокурора ґрунтується не на припущенні,

[134] Хомутов С. В. По вопросу различных подходов к оценке заключения эксперта. *Вестник Восточно-Сибирского института МВД России*. 2019. № 1 (88). С. 266.

[135] Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.03.2021).

а на всебічному, повному й неупередженому дослідженні всіх обставин[136].

Після проведення СКТЕ слідчий, прокурор зобов'язаний ознайомитися з її змістом і оцінити висновок експерта як необхідну умову його використання для обґрунтування обвинувального акту, яким завершується досудове розслідування. В основу цих найважливіших процесуальних документів можуть бути покладені тільки такі висновки експерта, спроможність і остаточна обґрунтованість яких не викликає ніяких сумнівів.

Слідчий повинен проаналізувати і оцінити результати СКТЕ, визначити місце висновку експерта в усій сукупності наявних доказів, зібраних у кримінальному провадженні, оцінити зроблені висновки й перевірити дотримання вимог закону щодо процедури отримання та оформлення результатів проведеного дослідження. Покладеними в основу проведеного дослідження та формулювання висновків спеціальними знаннями слідчий зазвичай не володіє, а за тими відомостями, які містяться у висновку експерта, важко оцінити його рівень компетенції.

Зазначимо, що закон не забороняє слідчому, прокуророві у разі необхідності, звернутись за консультацією до відповідного фахівця (приміром, у галузі інформаційних та комп'ютерних технологій), спеціальні знання якого допоможуть об'єктивно оцінити висновки, зроблені експертом за результатами проведення судової експертизи, їх доказове значення взагалі і для конкретного кримінального провадження, зокрема.

Допомога спеціаліста під час оцінки результатів СКТЕ може знадобитись при наявності в матеріалах кримінального провадження суперечливих висновків, коли результати судової експертизи суперечать іншим зібраним доказам і у разі недостатнього досвіду слідчого. У разі необхідності спеціаліст може порадити витребувати документи, що містять відомості довідкового характеру, дати письмові консультації зі спеціальних питань.

---

[136] Несінов О. М. Порушення процедури оцінки доказів. Прогалини в практиці застосування кримінального процесу. URL: https://protocol.ua/ua/advokat_nesinov_porushennya_protseduri_otsinki_dokaziv_progalini_v_praktitsi_zastosuvannya_kriminalnogo_protsesu/

Слідчі (розшукові) дії не завжди несуть в собі інформацію про факти та обставини, що мають значення для правильного вирішення кримінального провадження. Беручи участь у спільному аналізі речових доказів, слідів, документів під час досудового розслідування, спеціаліст допоможе усунути цю прогалину. Наприклад, в процесі допиту свідка – продемонструвати речові докази, пояснити результати СКТЕ з позиції доведеності чи недоведеності будь-якого факту, явища. На цьому етапі спільного аналізу ще є можливість виправити упущення і отримати докази.

При вивченні висновків експертів прокурор, який здійснює нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням (ч. 2 ст. 36 КПК), повинен з'ясувати, чи проведена СКТЕ на підставі та у визначеному ст. ст. 242-245 КПК порядку, належною особою, з'ясувати відповідні висновки експертів критеріям допустимості доказів, перевірити забезпечення процесуальних прав і законних інтересів учасників кримінального провадження, оцінити зв'язок висновків експертів з вмістом доказів, що встановлюють певні обставини предмета доказування, а також з іншими фактами, що мають значення для розгляду і вирішення кримінального провадження по суті, з'ясувати, чи не суперечать висновки експертів іншим доказам, в тому числі отриманим в результаті проведення інших експертиз.

Вивчаючи матеріали кримінального провадження перед зверненням з обвинувальним актом до суду, прокурор, припускаючи можливість призначення в суді тієї чи іншої судової експертизи (повторної, або додаткової СКТЕ, у т. ч. СКТЕ як складової комплексної експертизи), повинен звернути увагу на наявність в матеріалах кримінального провадження даних, що дозволяють це зробити, вжити заходи щодо їх проведення на момент розгляду справи в суді.

Дотримання процедури оцінки доказів під час судового розгляду є одним із важливих елементів досягнення умов справедливого правосуддя у кримінальному процесі. За змістом ч. 1 ст. 23 КПК України, суд першої інстанції під час судового розгляду повинен безпосередньо дослідити показання, речі і документи (допитати обвинуваченого, потерпілого, свідків, заслухати висновки

експертів, оглянути речові докази, оголосити протоколи та інші документи), оцінці підлягають лише ті докази, які були досліджені під час судового розгляду. Безпосередність сприйняття доказів дає змогу суду належним чином дослідити і перевірити їх (як кожний доказ окремо, так і у взаємозв'язку з іншими доказами), здійснити їх оцінку за критеріями, визначеними у ч. 1 ст. 94 КПК, і сформувати повне та об'єктивне уявлення про фактичні обставини конкретного кримінального провадження.

Висновок експерта за результатами проведення СКТЕ має велике значення при оцінці сукупності доказів у ході судового засідання, коли сторони, які беруть участь у судовому розгляді, подекуди ініціативно і на свій розсуд представляють докази в обґрунтування власної позиції і показують неспроможність протилежної[137].

О. В. Павлова виділяє в оціночній діяльності правовий, фактичний (змістовний) і тактичний компоненти і віддає перевагу правовій складовій, оскільки істотне порушення закону при отриманні об'єкта експертного дослідження, призначенні і проведенні експертизи тягне за собою визнання висновку експерта недопустимим доказом, нейтралізує його фактичне (змістовне) значення і не дозволяє розглядати різні тактичні прийоми його використання у доказуванні[138].

На нашу думку, загальну методику оцінки висновку експерта при проведенні СКТЕ слід розглядати як сукупність перевірочних дій і пов'язаних з ними розумових операцій, які виконує суб'єкт оцінки в оптимальній послідовності, керуючись при цьому вимогами кримінального процесуального закону, законами формальної логіки, використовуючи різні методи наукового аналізу, виробленої практикою у сфері інформаційних та комп'ютерних технологій.

Під час оцінки висновку експерта важливе з'ясування суб'єктивних чинників, що впливають на результати СКТЕ і остаточний висновок: чи встановив експерт умови утворення слідів або

---

[137] Варданян А. В., Грибунов О. П. Современная доктрина методико-криминалистического обеспечения расследования отдельных видов преступлений. *Вестник Восточно-Сибирского института МВД России*. 2017. № 2 (81). С. 32.

[138] Павлова Е. В. Методика оценки заключения эксперта прокурором – государственным обвинителем. *Библиотека криминалиста*. 2017. № 5. С. 213.

походження об'єктів, представлених на дослідження; чи застосував експерт обладнання, яке пройшло відповідну перевірку, і витратні матеріали, придатні за термінами виготовлення і умовами зберігання; чи застосував експерт методи, засоби і методики, рекомендовані для дослідження конкретних об'єктів; чи правильно їх використовував (оцінка наукової обґрунтованості висновку експерта); наскільки аргументовано і переконливо підтверджені висновки результатами експертного дослідження (обґрунтованість висновку експерта)[139]; чи правильно використано відомості, викладені у висновках інших експертів та ін.

Оцінка допустимості висновку експерта як доказу передбачає аналіз дотримання ним в ході експертного дослідження відповідних кримінальних процесуальних правил. Стосуються такі вимоги як висновку експерта, так і тих джерел доказів, які покладені в основу висновку за результатами СКТЕ. Вони мають відповідати загальним ознакам, властивим усім джерелам доказів, а також спеціальним, характерним тільки для електронних носіїв інформації. Зокрема, СКТЕ повинна проводитися компетентним фахівцем, огляд електронного носія інформації повинен здійснюватися відповідно до визначеної КПК процедури уповноваженими особами, хід і результати слідчої (розшукової) дії повинні бути зафіксовані у відповідному протоколі. З цієї позиції до електронних носіїв інформації повинні пред'являтися більш суворі вимоги, оскільки для їх оцінки необхідні спеціальні пристрої, особи, що володіють знаннями у вузькій сфері науки.

Не заперечуючи важливості оцінки правової складової оцінки висновку експерта при проведенні СКТЕ, відзначимо складність оцінки так званої змістовної (фактичної) його сторони. Адже проведення судової експертизи доручається особі, що володіє спеціальними знаннями, а оцінювати висновок експерта доводиться особі, яка не володіє цими знаннями. Це іще раз підтверджує доцільність використання допомоги спеціаліста, експерта.

Під час судового розгляду у кримінальному провадженні, де було проведено СКТЕ, також виникають певні труднощі з оцінкою

[139] Моисеева Т. Ф. Основы судебно-экспертной деятельности : конспект лекций. М. : РГУП, 2016. С. 81.

наукової обґрунтованості обраної експертної методики, правомірності її застосування в конкретному випадку, відповідності методики сучасним досягненням у відповідній сфері спеціальних знань, так як суд не є фахівцем і не володіє знаннями експерта. Алгоритм оцінки наукової сторони висновку експерта, дотримання якого є гарантією правильності його оцінки, полягає у з'ясуванні: науковості застосованих методів; можливості вирішити з їх допомогою коло експертних завдань, що стоять перед експертом; наявності у висновку експерта наукового пояснення отриманих ним результатів[140].

Чи не єдиною можливістю перевірки наукової обґрунтованості і достовірності висновку експерта є реальна змагальність експертів, яка досягається визначеною у КПК України можливістю сторін кримінального провадження клопотати про призначення судової експертизи. У такому випадку можна припустити, що висновки експертів «різних сторін» повинні мати протилежні (у всякому разі не співпадаючі висновки). Експерт займає процесуальне становище нейтральне, він не є ні стороною обвинувачення, ні стороною захисту. Неприйнятною є ситуація, коли дослідження одних і тих самих об'єктів для відповіді на аналогічне питання залежить від інтересів відповідної сторони, яку представляє «свій» експерт. При реальній змагальності експертів, залучених сторонами захисту та обвинувачення, право остаточного прийняття рішення фактично залишається за судом, вимушеним в судовому рішенні визнати ту чи іншу позицію правильною.

Достовірність криміналістичної інформації визначається її відповідністю відповідним явищам і процесам, а достатність – потребам у криміналістичній інформації суб'єкта доказування[141]. Найбільш важким завданням при оцінці висновку СКТЕ є завдання оцінки достовірності даного виду доказів. Пов'язано це з тим, що визначення достовірності висновку передбачає відповідний рівень

[140] Седова Т. А. Тактика назначения и производства судебной экспертизы. Криминалистика: учеб. / под ред. Т. А. Седовой, А. А. Эксархопуло. СПб., 2001. С. 599–600.

[141] Писарев Е. В., Золотов М. А. Оценка значимости криминалистической информации. *Вестник Волжского университета имени В. Н. Татищева*. 2018. № 2. Т. 1. С. 186.

знання слідчим предметної частини експертизи. Можливість слідчого, прокурора, слідчого судді і суду точно оцінювати наукову обґрунтованість висновку експерта є досі достатньою спірною, оскільки для цього необхідно володіти певним комплексом знань, близьких за рівнем до знань самого експерта, або здійснити оцінку обґрунтованості цього виду доказів за участю фахівця належного рівня[142].

На нашу думку, відображення у чинному КПК України права сторони захисту ініціювати призначення судової експертизи є єдиною можливістю перевірки наукової обґрунтованості і достовірності висновку експерта, залученого протилежною стороною кримінального провадження, у т. ч. слідчим, забезпечує реальну змагальність експертів.

Не заперечуючи твердження щодо необхідності підготовки уповноважених осіб зі спеціальних питань з метою правильної оцінки висновку експерта[143], варто звернути на очевидну недосяжність такого рівня знань більшістю з них у сфері інформаційних та комп'ютерних технологій. Адже, на жаль, через ускладнення висновків експерта у зв'язку із застосуванням високотехнологічних методів, засобів дослідження і обладнання, складних ілюстративних матеріалів у вигляді діаграм, таблиць, креслень, схем, ускладнилися й завдання оцінки висновку слідчим, прокурором, слідчим суддею, судом. Вказані суб'єкти мають можливості для оцінки висновку експерта як процесуальними способами (допит експерта судом з метою роз'яснення, уточнення та доповнення складеного ним висновку для усунення його незрозумілості або неповноти), так і непроцесуальними – без оформлення процесуальних документів (консультації спеціаліста, експерта).

Висновок експерта не є обов'язковим для особи або органу, яка здійснює провадження, але незгода з висновком експерта повинна бути вмотивована у відповідних постанові, ухвалі, вироку (ч. 10 ст. 101 КПК). Хоча закон і не встановлює переваги одних доказів перед іншими, проте вважаємо, що висновки експерта, за-

---

[142] Аверьянов Т. В. Судебная экспертиза. Курс общей теории. М. : НОРМА ИНФРА-М, 2014. С. 468.

[143] Сорокотягин И. Н., Сорокотягина Д. А. Судебная экспертиза : учебник и практикум для академического бакалавриата. М. : Юрайт, 2015. С. 141.

сновані на результатах проведених досліджень у галузі інформаційних та комп'ютерних технологій, часто носять більш об'єктивний характер, ніж докази особистісного і вербального характеру, приміром, показання підозрюваного.

На підставі проведеного аналізу висновку експерта за результатами СКТЕ, судом, як основної та, водночас, остаточної інстанції оцінки джерел доказів у кримінальному провадженні, можливе прийняття одного з таких рішень: визнання висновку повним і обґрунтованим; визнання висновку недостатньо повним і обґрунтованим (в такому разі можливе призначення додаткової експертизи, допит експерта в суді); визнання висновку необґрунтованим, що може спричинити призначення і проведення повторної експертизи.

Що стосується використання висновку експерта за результатами СКТЕ у кримінальному провадженні, то воно являє собою оперування ним суб'єктами доказування під час кваліфікації кримінального правопорушення, для встановлення фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню, а також для вирішення інших тактичних завдань у ньому.

Можемо резюмувати, що судова експертиза є найбільш кваліфікованою формою використання спеціальних знань у кримінальному провадженні. Під оцінкою висновку експерта за результатами СКТЕ розуміють: розумову діяльність слідчого, прокурора, слідчого судді і суду, в ході якої вони перевіряють відповідність закону усіх обставин, пов'язаних з призначенням цієї експертизи (вимоги до особи, яка залучена до її проведення, до постанови (ухвали) про доручення проведення СКТЕ, висновку (структура, зміст, реквізити, підписи та ін.)); перевірку матеріалів, представлених на експертизу (порядок отримання, посвідчення речових доказів, зразків для порівняльного дослідження (їх достатність); з'ясування повноти дослідження (чи всі об'єкти досліджувалися, чи на всі питання отримані відповіді); оцінку логічної обґрунтованості ходу і результатів дослідження, відповідність висновків проведеному дослідженню і його результатам.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Аверьянов Т. В. Судебная экспертиза. Курс общей теории. М.: НОРМА ИНФРА-М, 2014. 480 с.
2. Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма, 2001. 240 с.
3. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. К., 2008. с.
4. Бірюков В. В. Криміналістичне документознавство. К. : Паливода А. В., 2007. 331 с.
5. Бондар В. С., Солодовніков А. П., Дехтярьов Є. В. Розслідування розбоїв, вчинених організованими групами : навч.-метод. посіб. 2014. 276 с.
6. Варданян А. В., Грибунов О. П. Современная доктрина методико-криминалистического обеспечения расследования отдельных видов преступлений. *Вестник Восточно-Сибирского института МВД России*. 2017. № 2 (81). С. 23–34.
7. Виницкий Л. В., Мельник С. Л. Экспертная инициатива в уголовном судопроизводстве. М. : Экзамен, 2009. 382 с.
8. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М. : ООО «Юрлитинформ», 2001. 496 с.
9. Воронин С. А. Совершенствование методов современной судебной экспертизы. *Полицейская деятельность.* 2016. № 3. С. 323–328. DOI: 10.7256/2222-1964.2016.3.18655https://doi.org/10.7256/2222-1964.2016.3.18655.
10. Довженко О. Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету*. *Серія Право.* 2019. Вип. 55. Т. 2. С. 124–127.
11. Експертиза комп'ютерної техніки і програмних продуктів або комп'ютерно-технічна експертиза. URL: http://centrservis.com.ua/ekspertiza-kom p-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza (дата звернення: 03.02.2021).
12. Експертизи у судочинстві України : наук.-практ. посіб. / заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.
13. Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : методичні рекомендації. Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. 73 с.
14. Зачек О. І., Навроцька В. В., Федчак І. А. Особливості розкриття та розслідування кіберзлочинів : методичні рекомендації. Львів : Львівський державний університет внутрішніх справ, 2010. 60 с.
15. Зинин А. М. Теория судебной экспертизы : учебник для вузов / под ред. Е. Р. Россинской. М., 2013. 384 с.

16. Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий. *Вестник Казанского юридического института МВД России*. 2018. Т. 9. № 2. С. 274–278.

17. Зозуля Н. Особливості проведення експертизи комп'ютерної техніки, програмних продуктів відео- та звукозаписів. *Українське право*. URL: https://www.ukrainepravo.com/scientific-thought/legal_analyst/osoblyvosti-proved ennya-ekspertyzy-komp-yuternoyi-tekhniky-programnykh-produktiv-video-ta-zvu kozapys (дата звернення: 03.02.2021).

18. Ивин А. А., Никифоров А. Л. Словарь по логике. М., 1997. 384 с.

19. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: наказ Генеральної прокуратури України, МВС України, СБУ України, Адміністрації ДПС України, Мінфін України, Мінюст України № 114/1042/516/1199/ 936/1687/5 від 16 листопада 2012 р. URL: http://zakon2.rada.gov.ua/laws/ show/v0114900-12 (дата звернення: 03.02.2021).

20. Інструкція про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах : Наказ Міністерства юстиції України від 12 грудня 2011 р. № 3505/5 (в редакції наказу Міністерства юстиції України від 7 вересня 2015 р. № 1659/5). URL: https://zakon.rada.gov.ua/laws/show/ z1431-11 (дата звернення: 03.02.2021).

21. Інструкція про призначення та проведення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 03.02.2021).

22. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1 (9). С. 140–144.

23. Касаткин А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений : автореф. дисс. на соискание ученой степени канд. юрид. наук. М., 1997. 20 с.

24. Кіберполіція виявила хакера, який інфікував тисячі комп'ютерів із 50 країн світу. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vyyavyla-xakera-ya kyj-infikuvav-tysyachi-kompyuteriv-iz--krayin-svitu-761 (дата звернення: 03.02.2021).

25. Климчук М. П. Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, та особливості їх виявлення. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід*. К. : НАВС, 2020. С. 84–88.

26. Климчук М. П., Михайлов П. С. Судова комп'ютерно-технічна експертиза як спосіб виявлення корупційної складової при розслідуванні протиправного впливу на результати офіційних спортивних змагань. *Вчені записки ТНУ імені В. І. Вернадського.* 2020. Т. 31 (70). Ч. 3. № 2. С. 109–113.

27. Книш М. Як розвалюють комп'ютерно-технічні експертизи? URL: http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/yak-rozvalyuyut-kompyuternotehnichni-ekspertizi.html (дата звернення: 03.02.2021).

28. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України.* 2017. № 1 (88). С. 182–191.

29. Конвенція про кіберзлочинність, ратифікована законом від 7 вересня 2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 03.02.2021).

30. Коршенко В. А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jumalul juridic national: teorie i practica*. 2017. №. 2. С. 190–194.

31. Коршенко В. А., Щербаковський М. Г. Тактичні та організаційні особливості зняття інформації з транспортних телекомунікаційних мереж. *Криміналістика і судова експертиза :* міжвідом. наук.-метод. зб., присвяч. 105-річчю заснування судової експертизи в Україні. Київський НДІ судових експертиз; редкол.: О. Г. Рувін (голов. ред.) та ін. Вип. 63. К. : Вид-во Ліра-К, 2018. Ч. 1. 424 с.

32. Коршенко В. А. Проблема визначення об'єктів судової комп'ютерно-технічної експертизи. *Вісник Харківського національного університету внутрішніх справ*. 2000. С. 150–152. URL: http://nbuv.gov.ua/UJRN/ VKhnuvs_2000_Spets (дата звернення: 03.02.2021).

33. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : дис. … канд. юрид. наук : 12.00.09. Х., 2017. 20 с.

34. Коршенко В. А., Юхно О. О., Матюшкова Т. П., Гнусов Ю. В., Лисенко А. М., Мітрухов П. М., Фоміна Т. Г. Особливості розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій : науково-методичні рекомендації. Серія: Бібліотечка слідчого і детектива: проблеми кримінального процесу. Х. : Харк. нац. ун-т внутр. справ, 2019. 48 с.

35. Костин П. В., Кувычков С. И. Исследование магнитных носителей : учеб. пособие. Н. Новгород, 2002. 130 с.

36. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 03.02.2021).

37. Кувычков С. И. О современных проблемах проведения судебно-компьютерных экспертиз в ходе предварительного расследования. *Вестник Нижегородской академии МВД России*. 2016. № 2 (34). С. 293–298.

38. Легких К. В. Отримання стороною захисту для експертного дослідження зразків, які знаходяться в матеріалах кримінального провадження. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 2. С. 196–200.

39. Лежух Т. І. Застосування електронних доказів у справах про захист честі, гідності та ділової репутації. *Віче.* 2013. № 16. С. 13–15.

40. Маринин С. А. Правовые и организационно-тактические основы выявления, документирования и раскрытия преступлений, совершаемых в сфере незаконного игорного бизнеса с использованием компьютерной техники и Интернета : монография. Н. Новгород : НА МВД России, 2015. 185 с.

41. Менжега М. М. Криминалистические проблемы расследования создания использования и распространения вредоносных программ для ЭВМ : дисс. … канд. юрид. наук. Саратов, 2005. 238 с.

42. Методика расследовани хищений социалистического имущества. Изд. 4 / отв. ред. В. Г. Танасевич. М., 1980. 172 с.

43. Моисеева Т. Ф. Основы судебно-экспертной деятельности : конспект лекций. М. : РГУП, 2016. 190 с.

44. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук 6 12.00.09. К., 2005. 23 с.

45. Найдьон Я. Пошук та вилучення віртуальних слідів створення та поширення інформації порнографічного змісту 6/2019. *Підприємництво, господарство і право.* DOI https://doi.org/10.32849/2663-5313/2019.6.58.

46. Незалежний інститут судових експертиз. *Офіційний сайт.* URL: https://nise.com.ua/it-ekspertyza (дата звернення: 03.02.2021).

47. Несінов О. М. Порушення процедури оцінки доказів. Прогалини в практиці застосування кримінального процесу. URL: https://protocol.ua/ua/advokat_nesinov_porushennya_protseduri_otsinki_dokaziv_progalini_v_praktitsi_zastosuvannya_kriminalnogo_protsesu/

48. Одерій О. В., Корона С. О., Самойлов С. В. Тактика слідчого огляду комп'ютерних систем та їх елементів. Донецьк, 2010. 88 с.

49. Олиндер Н. В. К вопросу о доказательствах, содержащих цифровую информацию. *Юридический вестник Самарского университета*. 2017. Т. 3. № 3. С. 107-110.

50. Орлов Ю. К. Судебная экспертиза как средство доказывания в уголовном судопроизводстве : науч. изд. М. : Институт повышения квалификации РФЦСЭ при Минюсте России, 2005. 319 с.

51. Осика І. М. Поняття способу підробки документів, що використовуються при вчиненні злочинів у сфері підприємництва. *Право і Безпека*. 2005. Т. 4. № 6. С. 92–94. URL: http://nbuv.gov.ua/UJRN/Pib_2005_4_6_26

52. Официальный экзамен EnCE: Сертифицированный пользователь EnCase : учебное руководство. URL: http://computer-forensics-lab.org/pdf/encase_EnCE.pdf (дата звернення: 12.03.2021).

53. Павлова А. А. Процессуальные и методические основы назначения судебной компьютерно-технической экспертизы. *Политехнический молодежный журнал.* 2018. № 5. С. 1–13.

54. Павлова Е. В. Методика оценки заключения эксперта прокурором – государственным обвинителем. *Библиотека криминалиста*. 2017. № 5. С. 213–214.

55. Павлова Ю. С. Особливості збирання та процесуального закріплення електронних доказів у цивільному судочинстві. *Науковий вісник Херсонського державного університету*. 2017. Вип. 4. Т. 1. С. 76–80.

56. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. ... канд. юрид. наук : 12.00.09. Х. : Харківський національний ун-т внутрішніх справ, 2007. 335 с.

57. Пашнєв Д. В., Щербаковський М. Г. Методика розслідування злочинів у сфері використання комп'ютерів, систем і комп'ютерних мереж. Криміналістика : підручник: у 2 т.; за заг. ред. А. Ф. Волобуєва, Р. К. Степанюка, В. О. Малярової; МВС України. Х. : ХНУВС, 2018. Т. 2. Глава 33. С. 261–274.

58. Перякина М. П., Унжакова С. В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. *Сибирский юридический вестник*. 2019. № 3-861. С. 81–85.

59. Писарев Е. В., Золотов М. А. Оценка значимости криминалистической информации. *Вестник Волжского университета имени В. Н. Татищева*. 2018. № 2. Т. 1. С. 186.

60. Поляков В. В. Судебная компьютерно-техническая экспертиза средств мобильной радиосвязи. *Право*. С. 140–143.

61. Поляков В. В., Шебалин А. В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации. Барнаул, 2013. 284 с.

62. Полякова М. В., Рукавішников В. С., Шабля О. М. Особливості експертних досліджень файлових структур, типових для функціонування окремих інтернет-браузерів. *Теорія та практика судової експертизи і криміналістики.* 2014. Вип. 10. С. 526–532.

63. Порядок зберігання речових доказів стороною обвинувачення, їх реалізації, технологічної переробки, знищення, здійснення витрат, пов'язаних з їх зберіганням і пересиланням, схоронності тимчасово вилученого майна під час кримінального провадження : Постанова Кабінету Міністрів України від 19 листоп. 2012 р. № 1104. URL: https://zakon.rada.gov.ua/laws/show/1104-2012-%D0%BF (дата звернення: 03.02.2021).

64. Потапов С. А., Потапова И. С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. *Социально-экономические процесы и явления.* 2016. Т. 11. № 11. С. 155–161.

65. Предупреждение экспертных ошибок / под ред. Д. Я. Мирского, В. Ф. Статкуса, А. К. Педенчука. М., 1990. 75 с.

66. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/ show/851-15 (дата звернення: 03.02.2021).

67. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5 (дата звернення: 03.02.2021).

68. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. *Відомості Верховної Ради України.* URL: http://zakon2.rada.gov.ua/ laws/show/4038-12 (дата звернення: 03.02.2021).

69. Проблемы проведения и научного обеспечения судебных экспертиз. URL: https://ceur.ru/library/articles/ pravo/item127028.

70. Пчеліна О. В. Особливості огляду електронного документа. Актуальні питання розслідування кіберзлочинів : матеріали Міжнародної науково-практичної конференції. Х., 2013. С. 159–162.

71. Россинская Е. Н. Гносеологические и деятельностные экспертные ошибки при использовании в производстве судебных экспертиз современных технологий. *Вестник Московского университета МВД России*. 2015. № 3. С. 18–22.

72. Россинская Е. Р. Ошибки судебной экспертизы: классификация, выявление, предупреждение. *Союз криминалистов и криминологов*. 2014. № 2. С. 132–143.

73. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. *Право и закон.* М., 2001. 416 с.

74. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. 2-е изд., перераб. и доп. М. : Норма, 2008. 687 с.

75. Россинская Е. Р., Галяшина Е. И. Настольная книга судьи. Судебная экспертиза. М. : Проспект, 2010. 464 с.

76. Рувін О. Г. Судові експертизи в процесуальному праві України : навч. посіб. К. : Вид-во Ліра-К, 2019. 424 с.

77. Сабадаш Р. В. Судова комп'ютерно-технічна експертиза: правові підстави й особливості призначення. *Науковий вісник Чернівецького університету*. 2013. Вип. 660. С. 134–138.

78. Сальник С. В., Сторчак А. С., Крамський А. Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. *Системи обробки інформації*. 2019. № 2 (157). С. 121–128.

79. Седова Т. А. Тактика назначения и производства судебной экспертизы. Криминалистика : учебник / под ред. Т. А. Седовой, А. А. Эксархопуло. СПб., 2001. С. 572–604.

80. Сергеев М. С. Критерии доказывания электронных преступлений при применении мобильных приложений. Особенности их изъятия. *Актуальные проблемы экономики и права*. 2016. Т. 10. № 2. С. 264–272.

81. Сімакова-Єфремян Е. Б., Балинян Т. Є., Дереча Л. М. Про критерії оцінювання методик проведення судових експертиз в Україні. Теорія та практика судової експертизи і криміналістики : збірник наукових праць. Вип. 10. Х. : Право, 2010. 367 с.

82. Смолина А. Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дисс. … канд. техн. наук : 05.13.19 «Методы и системы защиты информации, информационная безопасность». Томский государственный университет систем управления и радиоэлектроники. Томск, 2017. 132 с.

83. Сорокотягин И. Н., Сорокотягина Д. А. Судебная экспертиза : учебник и практикум для академического бакалавриата. М. : Юрайт, 2015. 288 с.

84. Степанов В. В., Бабаков М. А. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий. М. : Юрлитинформ, 2014. 148 с.

85. Стефанчук Р. Інформаційні технології та право: quo vadis? *Право України*. 2018. № 1. С. 30.

86. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. Вип. 146. С. 179–190.

87. Судебная компьютерно-техническая экспертиза (экспертное заключение). Ошибки, связанные с производством экспертного исследования. URL: http://arbir.ru/articles/a_5102.htm

88. Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 18. 2 вер. С. 24–32.

89. Усов А. И. Концептуальные основы судебной компьютерно-технической экспертизы : дис. ... д-ра юрид. наук. М., 2002. С. 97–98.

90. Ухвала слідчого судді Вищого антикорупційного суду про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 30.09.2019 у справі № 760/24486/19 (кримінальне провадження № 42018000000002019). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

91. Ухвала слідчого судді Жмеринського міськрайонного суду про задоволення клопотання від 03.04.2019 у справі № 130/82/19 (кримінальне провадження № 12019020130000019). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

92. Ухвала слідчого судді Луцького міськрайонного суду Волинської області про відмову у задоволенні клопотання про призначення комп'ютерно-технічної експертизи від 26.07.2018 у справі № 161/11495/18 (кримінальне провадження № 1-кс/161/6086/18). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

93. Ухвала слідчого судді Новозаводського районного суду Чернігівської області про відмову у призначенні комплексної комп'ютерно-технічної експертизи від 18.12.2015 у справі № 751/6804/18. URL: https://conp.com. ua/search/lawsuit (дата звернення: 12.03.2021).

94. Ухвала слідчого судді Октябрського районного суду м. Полтави від 26.03.2019 у справі № 569/1173/19 (кримінальне провадження № 42019171010000004). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

95. Ухвала слідчого судді Приморського районного суду м. Одеси про призначення судової комп'ютерно технічної експертизи від 05.02.2019 у справі № 522/8682/18 (кримінальне провадження № 220181600000000053). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

96. Ухвала слідчого судді Рівненського міського суду Рівненської області про призначення судової комп'ютерно-технічної експертизи від 13.12.2018 у справі № 569/23518/18 (кримінальне провадження № 12018180010002477). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

97. Ухвала слідчого судді Рівненського міського суду Рівненської області про призначення судової комп'ютерно-технічної експертизи від 16.04.2019 у справі № 569/1173/19 (кримінальне провадження № 12018180000000335). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

98. Ухвала слідчого судді Самарського районного суду м. Дніпропетровська про призначення комп'ютерно-технічної експертизи від 24.05.2019 у справі № 206/2829/19 (кримінальне провадження № 12019040700000137). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

99. Ухвала слідчого судді Сєвєродонецького міського суду Луганської області про призначення судової комп'ютерно технічної експертизи від 22.03.2019 у справі № 428/3245/19 (кримінальне провадження № 12018130370002160). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

100. Ухвала слідчого судді Тернопільського міськрайонного суду Тернопільської області про призначення комп'ютерно-технічної експертизи від 17.10.2018 у справі № 607/21024/18 (кримінальне провадження № 12018210000000316). URL: https://conp.com.ua/search/lawsuit (дата звернення: 12.03.2021).

101. Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юрид. мир, 2007. 217 с.

102. Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2 (22). С. 97–100.

103. Хахановський В. Г. Можливості і перспективи використання інформаційних технологій в експертній практиці. *Криміналістика і судова експертиза*. 2017. Вип. 62. С. 330–344.

104. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Серія: Право*. 2017. № 4 (58). С. 80–85.

105. Хомутов С. В. По вопросу различных подходов к оценке заключения эксперта. *Вестник Восточно-Сибирского института МВД России*. 2019. № 1 (88). С. 264–274.

106. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112–124.

107. Шапошнікова І. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність. URL: https://ov-partners.com/osnovni-aspekty-vyboru-typu-i-provedennya-ekspertyzy-u-spravah-pro-kiberzlochynnist/?lang=ru

108. Шелупанов А. А., Смолина А. Р. Методика проведения подготовительной стадии исследования. Доклады ТУСУРа. 2016. Т. 19. № 1.

109. Шепітько В. Ю., Журавель В. А., Авдеева Г. К. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : монографія. Х. : Вид. агенція «Апостіль», 2017. 260 с.

110. Шепітько В. Ю., Коновалова В. О., Журавель В. А. Криміналістика : підручник. 4-е вид., перероб. і доп. Харків : Право, 2010. 464 с.

111. Шутемова Т. В. Оценка прокурором заключения судебного эксперта по уголовным делам. *Вестник Волжского университета имени В. Н. Татищева*. 2018. № 3. Т. 1. С. 191–198.

112. Щербюк Х. В., Пядишев В. Г. Одеський державний університет внутрішніх справ. *Особливості вилучення комп'ютерної техніки під час проведення обшуку.* С. 64–65.

113. Acronis TrueImage 7.0. URL: http://www.acronis.com/ru-ru/company/inpress/2004/09-04-ru-ixbt-trueimage-1-creating-image.html (дата звернення: 12.03.2021).

114. Good Practice and Advice Guide for Managers of e-Crime Investigation. URL: http://www.acpo.police.uk/documents/crime/2011/201103 CRIECI14.pdf (дата звернення: 12.03.2021).

115. Guidelines for Best Practices in Examination of Digital Evidence. Checklist for handling digital Image and Audio evidence (Инструкция по обращению с цифровыми изображениями и аудиодоказательствами) IOCE, December 2000. URL: http://ioce.org/fileadmin/user_upload/2000/ioce%202000 %20digital% 20image%20audio_checklist%20for%20handling%20digital %20evid.doc (дата звернення: 12.03.2021).

116. Sammons J., Brunty J. Mobile device forensics: threats, challenges and future trends. *Digital Forensics: Threatscape and Best Practices. Syngress*. 2015, 182 p.

ГЛОСАРІЙ

Абонент – споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі.

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створившим його користувачем або процесом).

Авторизований користувач (authorized user) – користувач, що володіє певними повноваженнями.

Адміністратор (administrator, administrative user) – користувач, роль якого включає функції керування КС і/або КЗЗ.

Безпека інформації (information security) – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Втрата інформації (information leakage) – неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

Дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки.

Доступ до інформації (access to information) – вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи.

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) – комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами.

Інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Комп'ютерна система; КС (computer system, target of evaluation) – сукупність програмно-апаратніх засобів, яка подана для оцінки.

Комп'ютерний вірус (computer virus) – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Користувач (user) – фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

Обчислювальна система; ОС (computer system) – сукупність програмних-апаратних засобів, призначених для обробки інформації; Автоматизована система.

Пароль (password) – секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації; Персональний ідентифікаційний номер.

Передавання даних – передавання інформації у вигляді даних з використанням телекомунікаційних мереж.

Провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням; Телекомунікаційна послуга (послуга) – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій.

Файл – порція інформації, що зберігається на комп'ютері та на яку є посилання. Файл може бути безструктурним, мати досить складну структуру або містити інші файли.

Додаток А

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
В ******** ОБЛАСТІ**
СЛІДЧЕ УПРАВЛІННЯ
*вул. **********, **, м. **********, індекс, т. (0**)***-**-*,*
****@****.gov.ua*

ПОСТАНОВА
про призначення комп'ютерно-технічної експертизи

м. ********** ** лютого 20 __ року

Слідчий відділу розслідування особливо тяжких злочинів Головного управління Національної поліції в ********** області капітан поліції Іванов Іван Іванович, розглянувши матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № 120********** від 01.01.2019 року за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 361-2 КК України, –

ВСТАНОВИВ:

До СУ ГУНП в ********* області надійшли матеріали відділу протидії кіберзлочинам в ********** області ДК НПУ про те, що в ході проведення оперативно-розшукових заходів встановлено, що житель м. ********** вчиняє злочинні дії з використанням електронно – обчислювальної техніки, а саме маючи певний досвід у сфері комп'ютерного програмування, зареєструвалась на форумах хакерського спрямування (в тому числі і закритих), з метою удосконалення набутих навичок та збуту шкідливого програмного забезпечення, а також інформації, отриманої за допомогою нього.

01.01.2019 року відомості про вчинення вказаного кримінального правопорушення внесені до Єдиного реєстру досудових розслідувань № 120********** за ч. 1 ст. 361-2 КК України.

Встановлено, що гр. Семенюк Семен Семенович 01.01.1991 р.н., який проживає за адресою: м. **********, вул. ******, **, через мережу інтернет, залишаючи повідомлення на інтернет форумах, збував користувачам логіни та паролі облікових записів громадян (аккаунти соціальних мереж, електронні поштові скриньки тощо).

01.02.2020 на підставі ухвали слідчого судді ******** міськрайонного суду проведено санкціонований обшук за місцем проживання Семенюка С.С. в м. ********** по вул. *********, **, під час якого було вилучено майно, що являється речовими доказами по кримінальному провадженні, адже були знаряддями кримінального правопорушення та зберегли на собі його сліди, а саме:

– системний блок із номером **********;

– системний блок, номер на материнській платі **********;

– ноутбук марки «Dell» серійний номер ********** із зарядним пристроєм;

– флешка марки «Kingston» із прикріпленим шнурком червоного кольору;

– флешка марки «Silicon Power» 16 Gb, із брелком у вигляді автомобіля;

– мобільний телефон марки «iPhone» imei: **********, укомплектований сім картою мобільного оператора «Лайф» та чохлом чорного кольору.

Відповідно ч. 1 ст. 243 КПК України, експерт залучається за наявності підстав для проведення експертизи за дорученням слідчого судді чи суду, наданим за клопотанням сторони кримінального провадження.

Беручи до уваги вищевикладене, та враховуючи те, що для вирішення суттєвих питань у даному кримінальному провадженні необхідні спеціальні знання, виникла необхідність у призначенні та проведенні комп'ютерно-технічної експертизи.

Враховуючи викладене, керуючись ст.ст. 110, 242, 243 КПК України, –

ПОСТАНОВИВ:

1. Призначити у кримінальному провадженні № 120 ********** від 01.01.2019 року за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 361-2 КК України комп'ютерно-технічну експертизу, до проведення якої залучити експертів ********** НДЕКЦ МВС України.

2. На вирішення експерта поставити питання:

1) чи міститься на носіях інформації наданих на експертизу об'єктах дослідження інформація стосовно логінів та паролів доступу до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів Інтернет-банкінгу та інших ресурсів і у якому вигляді?

2) які атрибути (час створення, редагування, видалення тощо) виявлених файлів, що містять інформацію стосовно логінів та паролів доступу до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів Інтернет-банкінгу та інших ресурсів, виявлених на носіях наданих на експертизу об'єктах дослідження?

*3) чи містять носії інформації наданих на експертизу об'єктів дослідження, сліди доступу до веб-ресурсів *****.ua, *****.com, ******.cc?*

4) чи містять носії інформації наданих на експертизу об'єктів дослідження програмне забезпечення, яке визначається антивірусним програмним забезпеченням експерта як шкідливе, якщо так то чи є сліди його використання чи розповсюдження?

5) чи містять носії інформації наданих на експертизу об'єктів дослідження збереженні в Веб-браузерах логіни та паролі, якщо так прошу її зберегти?

6) чи містять носії інформації наданих на експертизу об'єктів дослідження відомості про графічні файли, що містять напис «валид», «невалид»?

7) чи містять носії інформації наданих на експертизу об'єктів дослідження, історію браузера? Якщо так, то прошу її зберегти?

8) чи містять носії інформації наданих на експертизу об'єктів дослідження програмне забезпечення типу «чекер», «checker», яке за своїм функціоналом призначене для перевірки валідності логінів та паролів входу до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів Інтернет-банкінгу та інших ресурсів? Якщо так то чи наявні сліди використання вказаного програмного забезпечення?

9) чи містять носії інформації наданих на експертизу об'єктів дослідження файл з назвою «Зразок» із розширенням «.txt»?

10) чи містять носії інформації наданих на експертизу обєктів дослідження каталог з назвою «Telegram Dekstop», якщо так зберегти останній на оптичний носій інформації.

3. Надати експертам об'єкти дослідження, вилучені 01.02.2020 під час проведення обшуку за місцем проживання Семенюка С.С. в м. ************ по вул. ********, **, а саме: флешку марки «Kingston» із прикріпленим шнурком червоного кольору; флешку марки «Silicon Power» 16 Gb, із брелком у вигляді автомобіля, які поміщені до сейф-пакета № *********; мобільний телефон марки «iPhone» imei: ***************, укомплектований сім картою мобільного оператора «Лайф» та чохлом чорного кольору, який поміщено до сейф-пакета № ********.

4. Попередити експертів про кримінальну відповідальність за дачу завідомо неправдивого висновку, передбачену ст. 384 КК України, та за відмову експертів без поважних причин від виконання покладених на них обов'язків, передбачену ст. 385 КК України.

5. Постанову направити до ************** НДЕКЦ МВС України.

Слідчий ВРОТЗ СУ ГУНП
в ************ області
капітан поліції
Микола СИДОРЕНКО

ЗМІСТ

НАВЧАЛЬНЕ ВИДАННЯ

Климчук М. П.,
кандидат юридичних наук, доцент
Комісарчук Ю. В.,
кандидат юридичних наук, доцент
Марко С. І.,
кандидат юридичних наук, доцент
Стецик Б. В.,
кандидат юридичних наук

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Навчальний посібник

Видано в авторській редакції

Підписано до друку 28.12.2021.
Формат 60 × 84/16. Папір офсетний. Умовн. друк. арк. 6,51.
Тираж 100 прим. Зам. № 108-21.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.