

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ВНУТРІШНІХ СПРАВ  
Кафедра кримінального процесу, криміналістики та експертології  
факультет № 6**

**ТЕКСТ ЛЕКЦІЇ**

з навчальної дисципліни **«Криміналістичні засоби та методи розкриття і розслідування кримінальних правопорушень»** вибіркових компонент освітньої програми другого (магістерського) рівня вищої освіти спеціальність: 262 "Правоохоронна діяльність"

за темою: КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ЦИФРОВИХ ДОКАЗІВ  
(лекція № 2)

Харків 2023

## **ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Харківського національного  
університету внутрішніх справ  
Протокол № 7 від 30.08.2023 р.

## **СХВАЛЕНО**

Вченою радою факультету № 6  
Протокол № 7 від 25.08.2023 р.

## **ПОГОДЖЕНО**

Секцією науково-методичної ради  
ХНУВС з юридичних дисциплін  
Протокол № 7 від 29.08.2023 р.

Розглянуто на засіданні кафедри кримінального процесу, криміналістики та експертології факультету Протокол № 6 від 21.08.2023 року № 7

### **Розробник:**

Доцент кафедри кримінального процесу, криміналістики та експертології факультету № 6 кандидат юридичних наук, доцент Заяць Д.Д.

### **Рецензенти:**

Голова Київського районного суду м. Харкова, доктор юридичних наук, доцент Шаренко С.Л.

Професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор Степанюк Р.Л.

## План лекції

1. Фіксація цифрових (електронних) доказів.
2. Електронні (цифрові) докази в мережі Інтернет.
3. Загальний порядок вилучення комп'ютерної техніки та її зберігання.
4. Особливості вилучення мобільних пристроїв.
5. Призначення комп'ютерно-технічної експертизи.

## Рекомендована література:

### Основна

1. Криміналістика : підручник : у 2 т. Т. 1 / [А. Ф. Волобуєв, М. В. Даньшин, А. В. Іщенко та ін.] ; за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2018. – 384 с. – ISBN 978-966-610-231-0 (Т. 1). URL: <https://dspace.univd.edu.ua/xmlui/handle/123456789/6440>
2. Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. — 4-е вид., перероб. і доп. — Х.: Право, 2008. — 464 с. URL: <https://law.sspu.edu.ua/files/documents/books/library/17/shepitko.pdf>
3. Криміналістика : підруч. для студ. вищ. навч. закл. / [К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець, Ю. А. Чаплинська]. — 2-е вид, перероб. і доп. — Дніпро : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. — 480 с. URL: <https://er.dduvs.in.ua/bitstream/123456789/1191/1/%D0%9B%D0%95%D0%9A%D0%A6%D0%86%D0%87%20%D0%B7%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B8%202016%2B.pdf>
4. Криміналістика (криміналістична техніка): курс лекцій / П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков. Київ : МАУП, 2001. 216 с. <http://www.kul-lib.narod.ru/bibl.files/krim/book-710.htm>

### Додаткова

1. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. — Вид. 2-ге, доп. — Київ : Вид-во Нац. акад. внутр. справ, 2020. — 104 с. <http://elar.naiu.kiev.ua/bitstream/123456789/17605/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D1%85%20%28%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85%29%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D1%96%D0%B2.pdf>

### Інформаційні ресурси в Інтернеті

1. Експертна служба МВС України: <URL://dndekc.mvs.gov.ua/>
2. Харківський НДІ судових експертиз ім. Засл. проф. М.С. Бокаріуса: [URL:// www.hniise.gov.ua/](URL://www.hniise.gov.ua/)

## ТЕКСТ ЛЕКЦІЇ

### 1. Фіксація цифрових (електронних) доказів.

Складність сучасних комп'ютерних інформаційних систем, технологій обробки цифрових даних вимагає застосування техніко-криміналістичних засобів і технологій, які повинні забезпечити:

- унеможливлення запису будь-яких даних або здійснення інших змін на носіїві, що підлягає дослідженню на наявність слідів злочинної діяльності;
- максимальну універсальність підключення різних типів апаратних комп'ютерних засобів, периферійного устаткування;
- функціональну підтримку програмними засобами огляду комп'ютерних даних, визначення чи перевірки контрольних файлів, копіювання даних на фізичному рівні їх представлення і запису на іншому носіїві.

З технічної точки зору для фіксації доказів в електронній формі можна визначити два основні способи:

- фіксація на аналоговому матеріальному носіїві, властивості якого характеризуються безпосереднім і, як правило, відносно незмінним відображенням інформації (фото- та відеозапис);
- фіксація на комп'ютерному носіїві, фізичні властивості якого використовуються не для безпосереднього відображення інформації, а для запису-зчитування дискретних станів електромагнітного поля опосередковано через аналогово-цифровий перетворювач.

Безумовно, сьогодні створені й успішно використовуються у правоохоронній практиці різноманітні спеціалізовані апаратно-програмні комп'ютерні засоби для формування образів дисків та інших заходів комп'ютерної криміналістики, серед яких, наприклад, EPOS DiskMaster, Tableau TD3 Forensic Imager та багато інших. Але, нажаль, вони не досить розповсюджені в практичних правоохоронних підрозділах.

Тому для вирішення завдань найбільш розповсюдженої процесуальної дії щодо комп'ютерної техніки — огляду, в правоохоронній практиці, за статистикою, найчастіше застосовують відповідне типове програмне

забезпечення, більшість із яких не пов'язані з високою складністю і можуть бути використані правоохоронцями, які не мають глибоких технічних знань у сфері інформаційних технологій.

З огляду на це, для вирішення вказаних вище завдань пропонується використовувати дистрибутив операційної системи Ubuntu, пристосований для потреб провадження огляду локальних комп'ютерних засобів та віддалених ресурсів комп'ютерних мереж. Дистрибутив «Ubuntu cyber-crime» застосовується у вигляді ISO-файла. Нова версія дистрибутиву виходить двічі на рік.

Після запису цього ISO-файла на оптичний носій інформації DVD диск, який не підлягає перезапису, створюється Live-DVD варіант операційної системи, яка може відтворюватися в оперативній пам'яті комп'ютерного засобу і не залежить від наявності або відсутності жорсткого диска комп'ютера, не вносить будь-яких змін до цього носія, якщо він є, але робить можливим огляд інформації, вміщеної на всіх приєднаних до комп'ютера носіях.

До дистрибутиву входить стандартний для Ubuntu 16.04 набір програмного забезпечення, який доповнено:

1. Програмою для запису відеограм екрана монітора «XvidCap Screen Capture».
2. Програмою для підрахунку контрольних сум «Hash Checker».
3. Програмою для віддаленого керування операційними системами Windows «Tsclient 0.150» із підтримкою протоколу RDP (Remote Desktop Protocol — протокол віддаленого робочого столу).
4. Програмою автоматичного збирання інформації про апаратне і програмне забезпечення комп'ютерного засобу.
5. Програмою для форматування підключених носіїв.

З урахуванням слідчої ситуації, яка склалась, від носія інформаційної системи, електронний доказ та інші обставини, необхідно підібрати такі програмні засоби, які дозволили б вирішити поставлені завдання розслідування. Комплект програмного забезпечення, як правило, має бути остаточно відтворений у вигляді образу оптичного диска (файла з розширенням \*.iso,

\*.mdx, \*.nrg або інших поширених форматів), для якого необхідно визначити контрольну суму. Для забезпечення можливості підтвердження достовірності роботи програми підрахунку контрольних сум якій відводиться найважливіша роль засвідчення цілісності та автентичності зібраних доказів, необхідно створити файл-еталон.

З метою матеріалізації носія даних, запис образу оптичного диска необхідно здійснити мінімум у 2-ох примірниках на носії відповідного типу (CD або DVD), що не підлягають перезапису. Слід пам'ятати про те, що інформація, яка міститься навіть на неперезаписаному носії, може бути пошкоджена під час його використання. Один із примірників має бути контрольний, інший — робочий. Контрольний примірник диска необхідно упакувати так, щоб унеможливити доступ до нього, та опечатати стандартним шляхом. Інформацію про процедуру створення оптичних дисків та опечатування контрольного примірника необхідно внести до протоколу із зазначенням контрольної суми використаного образу оптичного диска.

Під час проведення слідчої дії використовується лише робочий примірник носія даних. Після завантаження операційної системи з Live-дистрибутиву необхідно створити файл, контрольну суму якого порівняти з контрольною сумою еталонного файлу, що відома заздалегідь.

Після того, як за результатами огляду будуть утворені окремі файли (скріншот, відеограма зображення монітора, образ носія та інші файли з орієнтувальною і доказовою інформацією), їх необхідно скопіювати у двох примірниках, створивши таким чином контрольний та робочий примірники отриманих доказів. Перед копіюванням цих файлів потрібно підрахувати їх контрольні суми, які внести до протоколу огляду. Контрольний примірник отриманих доказів необхідно упакувати так, щоб унеможливити доступ до нього, та опечатати стандартним шляхом, про що також зазначити у протоколі.

Таким чином, після закінчення слідчої дії, крім робочих примірників усіх програмних засобів, а також даних, що вміщують доказову інформацію, до протоколу також **обов'язково мають бути долучені:**

- контрольний примірник програмного засобу, що використаний для

виявлення, копіювання і записування досліджуваних даних на інший носій, а також контрольний примірник файла-еталона;

- контрольний примірник носія, що містить файли з доказовою інформацією;

- безпосередньо сам носій, що був об'єктом огляду (у разі наявності специфічних слідів, які потребують дослідження в лабораторних умовах).

Зазначені контрольні примірники повинні забезпечити можливість повторної (експертної) перевірки зафіксованих електронних доказів, у разі можливих сумнівів щодо їх цілісності, автентичності та ін.

Під час огляду місця події звертають увагу на апаратні об'єкти, які містять: персональні комп'ютери (настільні, портативні), периферійні пристрої, мережеві апаратні засоби (сервери, робочі станції, активне обладнання, мережеві кабелі тощо), інтегровані системи (органайзери, мобільні телефони, інші гаджети), вбудовані системи на основі мікропроцесорних контролерів, а також електронні носії даних: мікросхеми пам'яті, магнітні і лазерні диски, магнітооптичні диски, магнітні карти, флеш-пам'ять, пластикові картки та ін.

У випадку, коли слідча або оперативно-тактична ситуація вимагає невідкладного проведення огляду даних на комп'ютерному засобі, який був використаний для вчинення злочину, а його безпосереднє вилучення неможливе або недоцільне (наприклад, якщо комп'ютерний засіб неможливо вилучити фізично — він вбудований у сейф, його корпус закріплений таким чином, що для вилучення необхідно руйнувати частину приміщення, або таке вилучення призведе до значних матеріальних збитків для підприємства, банківської установи, або комп'ютер застосовується як хостінг-сервер, на якому зберігаються сайти сторонніх осіб, то такий огляд необхідно проводити з використанням дистрибутиву в порядку, розглянутому вище.

Спеціаліст з підрозділу кіберполіції повідомляє слідчого, учасників слідчої дії, понятих та присутніх про копіювання (зняття так званого дампу) оперативної пам'яті, браузера з історією, логінами, паролями, копіювання файлів месенджерів та даних щодо відомих мереж, до яких здійснювалося підключення, і паролів до них. Після цього з дозволу слідчого здійснюється

таке копіювання. При цьому спеціаліст кіберполіції повідомляє присутнім та учасникам слідчої дії про інформацію, яка підлягає копіюванню, її місцезнаходження на носії інформації, програмне забезпечення, за допомогою якого здійснюється таке копіювання, із зазначенням умов його ліцензування, зовнішнього носія інформації, на який здійснюється та в подальшому здійснюватиметься копіювання такої інформації, його серійних, ідентифікаційних чи інвентарних номерів.

Після завершення копіювання спеціаліст кіберполіції демонструє всім учасникам слідчої дії та присутнім на екрані адресу зовнішнього носія інформації, на який здійснено копіювання файлів, оголошує найменування та кількість скопійованих файлів, їхні розміри, після чого здійснюється від'єднання зовнішнього носія інформації від пристрою, з якого проводилося копіювання, та його упакування й опечатування биркою з коротким описом комп'ютерного обладнання, з якого було здійснено таке копіювання, із зазначенням на бирці облікового номера в протоколі обшуку.

У разі наявності інформації, яка підлягає доказуванню в кримінальному провадженні, необхідно доручити спеціалісту кіберполіції *зберегти скріншоти вікон та (або) файлів*. Спеціаліст кіберполіції повідомляє про обставини такого збереження, інформуючи учасників обшуку, присутніх та понятих усі виконані ним операції чи команди, які ним були здійснені для збереження таких скріншотів. Ця інформація заноситься до протоколу слідчої дії.

У разі необхідності, потрібно виготовити файл-образ усього жорсткого диска персонального комп'ютера (ПК) чи іншого комп'ютерного засобу, про що детально відобразити в протоколі слідчої дії із зазначенням:

- відомостей про жорсткий диск ПК, файл-образ якого необхідно створити;
- програмного забезпечення та умови ліцензування програмного забезпечення, за допомогою якого здійснюється таке копіювання;
- зовнішнього носія інформації, на який здійснюється таке копіювання, із зазначенням його ідентифікаційних ознак (серійних чи інвентарних номерів тощо);
- період часу, за який виготовлено такий образ жорсткого диска ПК.



Після завершення створення файл-образу спеціаліст кіберполіції демонструє учасникам слідчої дії, присутнім та понятим факт створеного образу, описує скопійовані файли із зазначенням їх властивостей, розміру та інших даних, про що вказується в протоколі.

Якщо екран пристрою заблоковано, за можливості слід з'ясувати пароль користувача, а також встановити, чи увімкнене шифрування диска. *Якщо пароль доступу не надається та є впевненість у тому, що шифрування диска не застосовується*, а присутнє лише блокування екрана, то слідчий доручає працівнику кіберполіції перезавантажити ПК та завантажитись у Live-режимі з будь-якого Linux-дистрибутиву, який після завершення завантаження надасть змогу переглядати та копіювати усю файлову систему даного ПК за допомогою провідника.

Якщо пароль доступу не надається та застосовується шифрування диска, то слідчий доручає працівнику кіберполіції виготовити дамپ оперативної пам'яті з метою відшукування паролів, що зберігаються у ній, до моменту вимикання. Для цього можуть бути застосовані або спеціалізовані апаратно-програмні засоби, наприклад, акселератор Tableau TACC1441, або окремі багатофункціональні та спеціалізовані програмні пакети й утиліти. Прикладом такого програмного засобу є, наприклад, «Multi Password Recovery, MPR» — багатофункціональна програма для Windows з розшифрування і тестування паролів на стійкість. Програма MPR автоматично знаходить і миттєво розшифровує паролі із більш ніж 110 популярних програм (FTP, E-mail клієнти, Інтернет пейджери, браузерери та ін.), не потребуючи при цьому втручання користувача. Крім розшифрування, MPR показує паролі під зірочками, дозволяє скопіювати SAM-файл (де зберігаються паролі адміністратора і користувачів ОС Windows, такий файл неможливо прочитати чи скопіювати стандартними засобами. MPR дозволяє скопіювати SAM файл для подальшої обробки альтернативними програмами), видалити збережені паролі, згенерувати новий пароль, зберегти звіти на диск. Усі свої дії та результати кожної операції працівником кіберполіції послідовно та детально повідомляються учасникам слідчої дії, присутнім, понятим та слідчому з метою повного, своєчасного та

якісного їх відображення в протоколі та/або додатках до нього. Після проведення слідчої дії, вилучені предмети, речі та документи в упакованому вигляді пред'являються всім учасникам, понятим та присутнім. Складається повний текст протоколу та додатків до нього, які надаються кожному учаснику для особистого ознайомлення та підпису. Оригінал носія інформації, на який здійснювався технічний запис перебігу та результатів проведеної слідчої дії, долучається до протоколу, про що в ньому робиться відповідний запис. У протоколі обов'язково повинно бути відображено конкретне місцезнаходження комп'ютера та його периферійного обладнання, обстановка та інші обставини, що можуть мати істотне значення для провадження. Слідчий повинен організувати забезпечення цілісності та збереження даних на ПК, які підлягають вимкненню з мережі живлення, для їх вилучення в ході проведення слідчої дії, а в разі неможливості вимкнення ПК з мережі живлення слідчий зобов'язаний організувати невідкладне копіювання даних в ході проведення слідчої дії (дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа).

Порядок фіксації комп'ютерних слідів на віддалених ресурсах *у мережі Інтернет*, загалом тотожний з описаним вище. Алгоритм дій відрізняється лише специфікою процесу доступу до ресурсів і програмного забезпечення, призначеного для виконання цього завдання. Предметом огляду також є комп'ютерна інформація, збережена або відтворена на носіях інформації, з'єднання з якими відбувається каналами телекомунікаційного зв'язку за правилами та технічними протоколами функціонування комп'ютерних мереж та мережі Інтернет. Слідчий зобов'язаний також вживати заходів щодо забезпечення надійного збереження даних щодо доступу до крипто-гаманців (логінів, паролів тощо) та крипто-валюти, яка міститься на крипто-гаманцях, виявлених на ПК, мобільних пристроях тощо в ході проведення слідчих дій.

## 2. Електронні (цифрові) докази в мережі Інтернет

Електронні докази в мережі Інтернет можуть міститися на веб-сайтах, електронній пошті, соціальних мережах, різноманітних форумах, у пошукових системах інформації тощо.

Здебільшого електронна інформація мережі Інтернет зберігається у вигляді веб-сторінок, які складаються з окремих електронних документів, що містять дані у вигляді тексту, графічних зображень, електронних таблиць, відео тощо і можуть бути переглянуті за допомогою спеціальних комп'ютерних програм — веб-переглядачів (браузерів): Internet Explorer, Mozilla Firefox, Google Chrome, Opera та ін. Сукупність веб-сторінок, об'єднаних за змістом та навігацією і розміщених за певною мережевою адресою, називається веб-сайтом (website).

Першим видом доказів, які можна отримати з **веб-сайта**, є його видимий, а другим, відповідно, невидимий зміст. Невидимий зміст — це мова програмування або його код (HTML, CSS, Javascript та ін.), що використовується для створення веб-сторінки, і фактичний зміст, який сервер направляє в браузер (програма для перегляду сайтів), а браузер його дешифрує і використовує для відображення вебсторінки на екрані.

Код сайта допомагає отримати електронні докази щодо особливостей фактичної інформації цього сайта.

Існують також *метадані*, які можуть бути джерелом високотехнічної інформації про саму веб-сторінку. Найпростіший приклад — інформація про дату останньої модифікації веб-ресурсу (веб-сторінки, зображення і т.д.).

Таку інформацію можна отримати за допомогою безкоштовного додатка FireBug для Google Chrome, а також інших аналогічних програм, наприклад, NetAnalysis®, яка розроблена спеціально для веб-браузера судово-медичної експертизи і підтримує всі основні настільні і мобільні браузери, проводить аналіз історії, кеш, куки тощо, має потужні можливості створення звітів, що дозволяє швидко отримувати докази, які стосуються діяльності користувача.

Це програмне забезпечення також має потужні аналітичні інструменти,

які допомагають розшифрувати і аналізувати дані.

«*BrowsingHistoryView*» — невелика безкоштовна програма, яка дає змогу отримати доступ до даних таких браузерів, як Internet Explorer, Mozilla Firefox, Google Chrome, Safari і відображає історію відвідування веб-сайтів у загальній таблиці. Утиліта надає інформацію про адресу відвідуваного сайту, його назву, дату і час відвідування, використовуваний браузер, профіль користувача тощо.

Додаток дозволяє проглядати історію відвіданих сторінок для будь-якого профілю користувача, зареєстрованого в системі. Є можливість експортувати отримані результати в CSV-, HTML- та XML-файл.

Важливе значення при розгляді електронних (цифрових) доказів у суді має їх достовірність. Тому, крім зберігання копії екрана (про що вже зазначалось раніше) на основі функції Print screen — PrtSc, для збереження даних веб-сторінки доцільно використовувати функцію браузера «Зберегти як», при виконанні якої зберігається код веб-сторінки.

Також здійснюється запис на телекамеру операції щодо відкриття сайту, при цьому одночасно відкривається певний відомий сайт, звідки фіксується дата та час перегляду. Можливе використання і спеціальних програм, які створюють записи екрана монітора.

Для пошуку інформації про реєстратора доменного імені сайту, провайдера, місця розміщення сайту (його IP-адреси), адміністратора сайту використовується система “Whois” — <http://Whois.com>. Для отримання вказаної інформації використовуються також інші програмні засоби, наприклад, [www.domaintools.com](http://www.domaintools.com), <http://centralops.net> тощо.

Знаючи IP-адресу комп'ютера підозрюваної особи та розуміючи правила надання доменних імен і хостингу, можна також, здійснивши зворотний пошук по Whois, побачити всі DNS/IP-записи, зареєстровані на зазначену особу. Існує можливість пошуку за іменем, за адресою електронної пошти, номером телефону або фізичною адресою.

Пошук за IP-адресою також дає змогу визначити країну, на території якої розміщений сайт, місто, геолокацію тощо (2ip.ua). За однією IP-адресою може знаходитися декілька сайтів (на одному комп'ютері розміщено декілька

програм).

Існують сервіси, наприклад, [whoer.net/ru](http://whoer.net/ru), які дають можливість переглянути всі сайти з однієї IP-адреси. Їх аналіз може надати додаткові відомості, необхідні для розслідування.

Водночас існує можливість фізичного розміщення сайта (хостінг) в іншому від провайдера місці та навіть в іншій країні. Для його визначення необхідно звертатися до провайдера — адже він здійснює відповідні налаштування.

**IP-адресу конкретного комп'ютера**, який працює під управлінням системи Windows7, можна отримати, якщо зайти в «Панель управління», вибрати закладку «Мережа та Інтернет», потім вибрати пункт «Інтернет підключення по локальній мережі», в якому в підпункті «Відомості» міститься інформація про IP-адресу цього комп'ютера. За допомогою сервісу <http://www.bravica.net/ru/netprovider.html>, <https://whoer.net/ru>, [2ip.ua](http://2ip.ua) можна визначити провайдера (Internet Service Provider, ISP) , що надає інтернет-послуги.

**Для ідентифікації IP-адреси конкретного веб-сайта** можна використати утиліту Ping або скористатися сервісом [2ip.ua](http://2ip.ua).

Залежно від версії операційної системи, існують кілька способів її виконання. Найпростіший спосіб, наприклад, у версії Windows7 — натиснути клавіші «Windows»+R, після чого ввести команду ping пробіл та адресу сайту, а потім натиснути клавішу «Enter».

Також для отримання детальної інформації про користувача мережі, адміністратора сайту, реєстратора доменного імені тощо необхідно надіслати відповідний запит провайдеру послуг або, якщо електронні дані знаходяться в юрисдикції іншої держави, необхідно надіслати запит (клопотання) про міжнародну правову допомогу та отримати, наприклад, номер телефону доступу, фізичну адресу, ім'я адміністратора ресурсу тощо. Підстави та умови надання правової допомоги та процедура написання запитів детально розглянута у Методичних рекомендаціях щодо виконання вимог міжнародних договорів та КПК України про міжнародну правову допомогу при проведенні

процесуальних дій у кримінальному провадженні від 20 квітня 2017 р., розміщених на сайті Генеральної прокуратури України (<http://www.gp.gov.ua> для зареєстрованих користувачів).

На практиці слідчому доводиться мати справу з об'єднанням різних сервісів, наприклад, електронні докази можуть міститися в інтернет-магазині, для реєстрації в якому використовується аккаунт соціальної мережі Facebook, оплата здійснюється через онлайн банкінг Приват24, а інформація надсилається користувачам Twitter або SMS-повідомлення, тобто електронні докази знаходяться на різних сервісах і в різних провайдерів. Подібні приклади зустрічаються досить часто, проте збирання доказів із різних джерел, незважаючи на певну складність, може бути більш продуктивним, ніж отримання доказів з одного місця.

Електронні докази можна *отримати із соціальних мереж*. Для слідчого корисною може стати інформація про *ідентифікатор підозрюваного (ID)*, а також інформація з листування користувачів та інша інформація, наприклад, зображення, які викладаються користувачами, оскільки вони можуть містити метадані з інформацією про дату та час створення зображення, місце його створення тощо.

Ідентифікатори використовують також і в мережі он-лайн-реклами, приміром, Google. Знаючи ідентифікатор, шляхом надсилання запиту, наприклад до адміністрації банерної мережі про здійснені грошові перекази, можна встановити конкретну фізичну чи юридичну особу, яка замовляла рекламу.

**Chat room.** Правопорушники досить часто використовують технологію багатокористувацьких конференцій (дискусій) реального часу в текстовому режимі через мережу Інтернет — IRC (англ. Internet Relay Chat). Хоча існують тисячі електронних каналів для дискусій, де обговорюються музика, політика, спорт тощо, злочинці можуть використовувати їх для обговорення свого сексуального досвіду, розміщення порнографічних матеріалів, установа зв'язків із неповнолітніми з подальшим залученням їх до надання сексуальних послуг у реальному світі тощо. У такій ситуації доцільно:

- установити назву Chat room;
- з'ясувати «Нік» зловмисника;
- визначити IP-адресу зловмисника;
- роздрукувати діалог зловмисника з потенційною жертвою;
- зберегти електронну копію зображення вікна комп'ютера.

Для фіксування повідомлень у чаті корисним може бути застосування сервісу Simkl (<http://simkl.org>), який дає змогу використовувати проміжний сервер для відповідних підключень.

Правопорушники найчастіше використовують для спілкування такі месенджери як Skype, Viber та інші. Ідентифікувати співрозмовника Skype можна за допомогою спеціальних програм, наприклад, Wireshark ([www.wireshark.org/download.html](http://www.wireshark.org/download.html)) або Skypesolver ([www.skresolver.com](http://www.skresolver.com)). Дізнатися IP-адресу абонента Viber, аналогічно як і у випадку зі Skype, можна за допомогою Wireshark. Для цього слід також застосувати Viber Desktop (<http://viber.com/desktop>).

**Електронні листи.** Злочинці дуже часто застосовують електронні листи для шахрайських схем, спаму, здирництва, шантажу, зараження комп'ютерів вірусами тощо. У таких випадках у потерпілих з'ясовують хто є Інтернет-провайдером, чи існує роздруківка електронного листа та чи збережена копія листа в комп'ютері, яка електронна адреса правопорушника.

Часто вдається виявити злочинця через IP-адресу, яка міститься у заголовках (header) Інтернет-повідомлень, що утворюються при їх передачі.

У таких заголовках міститься інформація про ISP, IP-адресу, дату та час створення повідомлення. Доступ до технічних заголовків електронного листа здійснюється через меню поштового клієнта, який використовується.

Для отримання таких даних необхідно зберегти на накопичувачу електронне повідомлення та надати його Інтернет-провайдеру або в Департамент кіберполіції Національної поліції України для проведення відповідних процесуальних дій.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано)

можна за допомогою сервісу <https://www.readnotify.com/>.

Злочинці намагаються унеможливити виявлення їх справжніх електронних адрес. Для цього вони використовують різні технології забезпечення анонімності роботи в мережі, а також програми безпечної передачі інформації. Ця обставина ускладнює встановлення місцезнаходження контактної особи. Серед головних способів забезпечення анонімності можуть застосовуватись: – проксі-сервери (HTTP, SOCKS 5 тощо); – VPN-сервери; – TOR та 2IP.

Останнім часом, особливо після блокування російських соцмереж, популярним стало використання VPN-серверів, за допомогою яких забезпечується конфіденційність інформації і приховування IP-адреси користувача. Тому, якщо користувач увійде у «VPN», то зможе дійти тільки до IP-адреси мережі «VPN», але не побачити початкової IP-адреси користувача.

Часто для заплутування слідів злочинці використовують заміну схожих букв в електронних адресах, наприклад, цифра «1» замість латинської літери «l», цифра «0» замість букви «o» тощо. Тому при підготовці запитів до Інтернет-провайдерів потрібно правильно вказувати назви сайтів та адреси електронної пошти, уважно дослідивши і вичитавши їх перед цим.

Для ідентифікації підозрюваного в мережі Інтернет часто необхідно визначити його аккаунт (обліковий запис) у певному Інтернет-сервісі, який зазвичай передбачає введення логіна та пароля).

Маючи аккаунт підозрюваного, необхідно ідентифікувати особу того, хто використовував цей аккаунт під час вчинення правопорушення (адже справжній власник аккаунта міг знаходитися в іншому місці).

У багатьох випадках обмін інтернет-повідомленнями (як злочинців між собою, так і злочинців із потерпілими) не завжди очевидний. Для дослідження таких повідомлень залучають фахівця, оскільки їх можуть знищити як потерпілий, так і злочинець. Проте за допомогою спеціального програмного забезпечення вони відновлюються.

Найпростіше виявити підозрюваного за його реальною e-mail адресою. Проте найчастіше злочинців відстежують через IP-адресу електронних



повідомлень. Ці адреси містяться в заголовках кожного інтернет-повідомлення.

Тільки один користувач може мати певну адресу в певний проміжок часу. ISP може ідентифікувати аккаунт, з якого вчинено правопорушення.

**Викрадення аккаунтів.** Для вчинення правопорушень злочинці часто послуговуються викраденими аккаунтами (так само як і грабіжники користуються викраденими автомобілями для втечі).

Для цього використовують такі способи:

– "троянський кінь". Злочинець надсилає повідомлення із заманливою інформацією (ліки за доступними цінами, як зменшити вагу тощо), в якому міститься комп'ютерний вірус. Пізніше цей вірус отримує необхідні паролі та направляє їх злочинцю;

– шантаж або викрадення. Злочинець надсилає листа від імені провайдера або банку та вимагає надати йому відповідні дані для поновлення аккаунту або доступу до мережі Інтернет.

Отримавши ці дані, зловмисник використовує їх для вчинення злочинів від імені невинної особи, тобто іноді, навіть коли існують певні електронні докази, дуже непросто встановити фізичну особу, яка вчинила комп'ютерний злочин через мережу Інтернет. Найчастіше все, що відомо про підозрюваного, — це його ІР-адреса, MAC-адреса, адреса електронної пошти, доменне ім'я або інтернетпсевдонім — «нік». Щоб ідентифікувати фізичну особу за ІР-адресою, фахівцям потрібні дані, які знаходяться в розпорядженні постачальника інтернет-послуг.

Постачальники інтернет-послуг (електронної пошти, хостінгових послуг) часто є єдиним джерелом інформації, яка дає змогу встановити зв'язок між віртуальною особистістю правопорушника і конкретною фізичною особою.

Тому незалежні власники даних часто виявляються ключовою ланкою в розслідуванні злочинів.

Отримавши аккаунт підозрюваного, необхідно з'ясувати хто реально проживає за вказаною адресою та хто отримує традиційну пошту.

Крім того, потрібно отримати список телефонних дзвінків із цієї адреси для з'ясування можливого контакту з інтернет-провайдером, а також визначити,

де здійснювався вхід в аккаунт у той час, коли вчинено правопорушення.

Для ідентифікації підозрюваного використовується кілька методів:

1) простежуються надходження коштів. У разі інтернет-шахрайства необхідно дослідити місце надходження коштів, наприклад картковий рахунок у банку;

2) відслідковуються надходження товарів. За купівлі товарів з використанням викрадених пластикових карток необхідно простежити місце надходження замовлених речей;

3) у провайдера мобільного зв'язку з'ясовується інформація про телефонні дзвінки. Для отримання інформації від зарубіжних провайдерів варто використовувати можливості контактного пункту "24/7" Департаменту кіберполіції Національної поліції України.

### **3. Загальний порядок вилучення комп'ютерної техніки та її зберігання.**

При обшуках, пов'язаних із вилученням комп'ютерної техніки, магнітних носіїв та інформації, виникає низка питань, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати дії злочинців із метою знищення комп'ютерної інформації. Наприклад, вони можуть використати спеціальне обладнання, яке в критичних випадках утворює сильне магнітне поле, що знищує магнітні записи. З метою запобігання непорозумінням у майбутньому бажано під час вилучення носіїв інформації отримати контрольні суми їх вмісту та обов'язково вказати їх у протоколі.

Під час вилучення комп'ютерів їх слід упаковувати в полімерні пакети, де горловина пакета міцно обв'язується шовковою (капроною) ниткою і фіксується двома подвійними простими вузлами. Вузли розміщують на діаметрально протилежних сторонах, на які клеється бирка, що містить написи з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якій вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім'ям та по батькові, особистим

підписом слідчого та прізвищами, іменами та по батькові, особистими підписами понятих, присутніх під час вилучення і пакування, скріпленими печаткою.

Не можна використовувати стрейч-плівки та плівкову стрічку з клейовим покриттям для пакування і закріплення паперових бирок із пояснювальними написами. Необхідно пронумерувати всі носії інформації, а також пакети, в які вони запаковані, проставити відповідні знаки на паперових аналогах інформації.

У протоколі слід вказувати серійні номери всіх вилучених блоків та їх балансові номери (за відповідною документацією бухгалтерії підприємства, установи, якщо вона наявна). Якщо номери повністю відсутні, треба докладно описати кожний блок відповідно до його індивідуальних ознак.

Для вилучення носіїв їх необхідно упакувати у жорстку негнучку коробку та опечатати її. Усі з'єднання сторін (клапанів) коробів повинні бути обклеєні паперовою стрічкою клейовим способом та скріплені печаткою.

У певних випадках можна використовувати й полімерні пакети, але з огляду на можливість несанкціонованого розрізання пакета за донну частину та потім заварювання його наново, у цьому разі необхідно обов'язково прошивати не тільки саму лише горловину пакета, а й донну його частину.

Потім необхідно зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість).

Коробка з носіями і опис поміщаються в поліетиленовий пакет, де горловина пакета міцно обв'язується шовковою (капроною) ниткою і фіксується двома подвійними простими вузлами, які розміщують на діаметрально протилежних сторонах.

Кожна упаковка повинна опечатуватися биркою, посвідченою написами з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якій вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім'ям та по батькові, особистим підписом слідчого та прізвищами, іменами та по батькові, особистими підписами

понятих, присутніх під час вилучення і пакування, скріпленими печаткою.

В окремих випадках, коли необхідно більш детально дослідити пристрої аудіо-, відео-, фотофіксації, спеціалізовані комп'ютери з нестандартним обладнанням (з платами шифрування, застарілими контролерами тощо), пристрої вводу-виводу інформації та ін., слід також вилучати дане обладнання. При цьому може знадобитися відповідний спеціаліст або певні технічні засоби.

Вилучення комп'ютерних засобів повинно проводитись в один прийом.

При перевезенні комп'ютерних засобів необхідно унеможливити їх механічні пошкодження і взаємодію з хімічно активними речовинами. Слід екранувати від впливу магнітних полів як комп'ютерні пристрої, так і магнітні носії. Такий вплив може призвести до пошкодження чи знищення інформації шляхом розмагнічування.

При розміщенні вилучених об'єктів на зберігання слід дотримуватися встановлених правил зберігання і складування електронних технічних засобів. Не можна ставити системні блоки у штабель вище трьох штук, а також розміщати на них будь-які інші предмети. Зберігають комп'ютери і комплектуючі у сухому, теплому приміщенні.

Недопустимо надання вилучених засобів у розпорядження підрозділу поліції, прокуратури, іншої організації (установи) з причин «виробничої необхідності», адже в процесі їх роботи можуть бути внесені зміни у файли інформації чи програми. Такі дії можуть призвести до пошкодження чи знищення електронних доказів. Тому неприпустимими є випадки використання вилучених як речові докази комп'ютерних засобів слідчими і оперативними працівниками для складання процесуальних документів, звітів тощо.

#### **4. Особливості вилучення мобільних пристроїв.**

Вилучення мобільних пристроїв iOS Apple (iPhone, iPad, iPod).

Доцільним є вилучення мобільного пристрою не в заблокованому вигляді або під час виконання власником мобільного пристрою лише вихідного дзвінка.

Під час вилучення мобільного пристрою в незаблокованому стані слідчий зазначає у протоколі слідчої дії спосіб вилучення мобільного пристрою, його

місцезнаходження, потім за участю працівника кіберполіції зазначає:

- найменування, марку та модель мобільного пристрою, місце його виявлення або особу, в якій він був фактично вилучений та за яких обставин;
- ідентифікаційні ознаки IMEI, серійний номер, із зазначенням способу ідентифікацій IMEI та серійного номера (напис на пристрої, електронна інформація під час натискання комбінації клавіш \*#06# тощо);
- інформація про те, що (у разі вилучення незаблокованого мобільного пристрою) на момент вилучення такий пристрій є незаблокований та відобразити виконані працівником кіберполіції дії з увімкнення режиму польоту та вимкнення WiFi і Bluetooth;
- перебіг та результати копіювання всього вмісту пристрою, із зазначенням всіх виконаних працівником кіберполіції дій, включаючи інформацію, що підлягає копіюванню, програмного забезпечення, за допомогою якого здійснюється таке копіювання, відомості про його ліцензування, носій інформації, на який здійснено копіювання наявної на мобільному пристрої інформації, із зазначенням ідентифікаційних номерів носія інформації (серійний чи інвентарний номер тощо).

У разі вилучення мобільного пристрою із заблокованим екраном роблять усе можливе, аби не дати його вимкнути, та вживають наступних заходів:

- доручають працівнику кіберполіції негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що зазначають в протоколі із описом часу виконання таких дій;
- якщо увімкнути режим «політ» та вимкнути WiFi і Bluetooth не вдається, здійснюють відповідний запис у протоколі. У такому разі доручають працівнику кіберполіції загорнути пристрій у шість шарів харчової фольги та під'єднати до джерела живлення (мобільна батарея тощо) для уникнення його вимкнення, про що зазначають в протоколі з описом часу виконання таких дій;
- звертають увагу на наявність персональних комп'ютерів, планшетів тощо у місці проведення обшуку та в разі встановленого на них програмного забезпечення iTunes доручають кіберполіції оглянути їх із метою виявлення резервної копії даних мобільного пристрою разом із паролем доступу;

– у разі повідомлення працівника кіберполіції про наявність на виявленому в місці проведення обшуку персональному комп'ютері резервної копії даних мобільного пристрою разом із паролем доступу заносять відповідні відомості до протоколу та доручають працівнику кіберполіції здійснити копіювання такої інформації.

Перебіг та результати з копіювання підлягають внесенню до протоколу, зокрема мають бути відображені відомості про:

- працівника кіберполіції, якому доручено здійснення копіювання інформації;
- програмне забезпечення, яке використовуватиметься для копіювання інформації;
- зовнішній носій інформації, на який здійснюватиметься таке копіювання, із зазначенням усіх ідентифікаційних даних такого носія інформації (серійний або інвентарний номер), із зазначенням файлів, які були скопійовані із зазначенням їх властивостей, які повідомляє працівник кіберполіції слідчому для внесення відповідних відомостей до протоколу.

У випадках виявлення пристрою у рідині, то його залишають, вилучають, упаковують та зберігають у рідині, місце і час вилучення такого пристрою зазначають у протоколі. Слід пам'ятати, що недопустимо контактування таких пристроїв з повітрям, оскільки це може призвести до окислення елементів та, як наслідок, його псування.

У разі виявлення мобільних Android пристроїв (Samsung, Huawei, Sony, Lenovo, LG, Meizu, Xiaomi тощо) насамперед роблять усе, аби вилучити пристрій із незаблокованим екраном і не дати його заблокувати або, що найгірше, вимкнути чи зашифрувати.

За можливості вилучають пристрій до блокування екрана або під час здійснення дзвінка, тільки вихідного, оскільки при вхідному дзвінку (в тому числі вхідному виклику у Viber, Telegram, What'sUp) пристрій не вимагає у власника зняття блокування екрана.

Працівнику кіберполіції доручають вимкнути автоблокування екрана в налаштуваннях, а в разі вимоги уведення коду доступу, переходять до розділу

часу автоблокування та обирають максимальний термін автоблокування, про що зазначають у протоколі слідчої дії.

У позитивному випадку отримання доступу до незаблокованого екрана, працівнику кіберполіції доручають негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що вносять відповідні записи до протоколу із зазначенням часу виконання таких дій.

Із залученням працівника кіберполіції копіюють увесь вміст пристрою, зазначивши точну послідовність дій у протоколі обшуку. Працівник кіберполіції повідомляє слідчому детальний опис проведених дій та наголошує для внесення у протокол тип пристрою (його ідентифікаційних ознак) та програмного засобу (відомості про його ліцензування), за допомогою якого знято копію.

У разі, якщо пристрій вилучено із заблокованим екраном, доручають працівнику кіберполіції негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що зазначають у протоколі із описанням часу виконання таких дій. Якщо увімкнути режим «політ» та вимкнути WiFi і Bluetooth не вдається, загортають пристрій у шість шарів харчової фольги та під'єднують до джерела живлення (мобільної батареї тощо) для уникнення його вимкнення, про що зазначають у протоколі.

Якщо фольги немає, для запобігання видаленню інформації віддаленим способом його вимикають.

Також працівнику кіберполіції доручають оглянути наявний на об'єкті ПК, планшет тощо із метою виявлення наявності у браузері збережених паролів та логінів облікового запису Playmarket Google, на якому можуть зберігатись резервні копії усього вмісту мобільного пристрою.

У разі наявності такої інформації працівник кіберполіції повідомляє про це всіх учасників слідчої дії та понятих, після чого, за дорученням слідчого здійснює копіювання наявної інформації, про що повідомляє всіх учасників слідчої дії, зокрема про наявність відповідної інформації, місця (адреси) її зберігання на персональному комп'ютері; програмного забезпечення, за допомогою якого здійснюватиметься копіювання; з'ємний носій електронної

інформації, на який здійснюватиметься копіювання (його серійний або ідентифікаційний чи інвентарний номер).

Після завершення копіювання працівник кіберполіції демонструє учасникам обшуку та понятим факт збереженості скопійованої інформації на зовнішньому носії інформації, повідомляє про її обсяг, назви файлів, які були скопійовані.

Далі здійснюють від'єднання зовнішнього носія інформації з персонального комп'ютера, його упакування та опечатування паперовою биркою з написом про персональний комп'ютер, з якого було здійснено копіювання інформації, короткий опис скопійованої інформації, серійний номер з'ємного носія інформації, підпис особи, якій належить персональний комп'ютер, підпис працівника кіберполіції, підписи понятих. Про все це роблять запис у протоколі.

Якщо пристрій знайдено в рідині — залишають, вилучають та транспортують його в рідині. Доручають працівнику кіберполіції витягти з пристрою акумулятор, не виймаючи з рідини. Забезпечують зберігання в рідині вилученого такого пристрою до моменту огляду, експертизи для унеможливлення контактування з повітрям, подальшим окисленням та, як наслідок, псуванням.

Якщо пристрій щойно кинуто в рідину або його кинули в рідину під час початку обшуку, в присутності працівників поліції тощо, доручають працівнику кіберполіції негайно витягти його з рідини, від'єднати акумулятор та просушити паперовими серветками, рушником, феном тощо.

Усі зазначені вище відомості підлягають обов'язковому занесенню до протоколу слідчої дії.

Вилучені мобільні пристрої (телефони, планшетні комп'ютери, GPSнавігатори, smart-годинники, портативні відеореєстратори тощо) упаковуються в окремі непрозорі пакети, що унеможливорює увімкнення пристрою в упаковці. Потім здійснюється їх опечатування біркою із зазначенням підписів: особи, в якій вилучається така інформація, працівника кіберполіції, який здійснив таке копіювання та понятих.



Разом з мобільним пристроєм необхідно, за можливості, вилучати та упаковувати також їх пристрої живлення. Спосіб упакування повинен забезпечувати неможливість підміни або зміни об'єктів дослідження, носіїв з об'єктами дослідження, зберігання від пошкодження, псування, погіршення або втрати властивостей, завдяки яким вони мають доказове значення.

## **5. Призначення комп'ютерно-технічної експертизи.**

За результатами проведених слідчих дій у ході досудового слідства та судового розгляду справи призначається комп'ютерно-технічна експертиза.

*Комп'ютерно-технічна експертиза (КТЕ)* це один з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації, а метою такої експертизи є пошук і закріплення доказів. Вона є комплексом дій, виконуваних професійно підготовленими експертними працівниками, що спрямований на дослідження та аналіз автоматизації інформаційних процесів, комп'ютерної техніки, електронних носіїв, так чи інакше пов'язаних з кримінальним провадженням.

Комп'ютерно-технічна експертиза призначається з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення та вивчення його ролі у правопорушенні, яке розслідується, а також отримання доступу до машинних носіїв інформації з подальшим її дослідженням.

Комп'ютерно-технічна експертиза по кримінальному провадженню може бути призначена слідчим (у рамках досудового розслідування) або судом і доручається конкретному експерту або експертній установі, за результатами якої складається висновок експерта, що служить доказом у справі.

Порядок здійснення КТЕ визначений наказом МВС України від 17 липня 2017 р. № 591, яким затверджена "Інструкція з організації проведення та оформлення експертних проваджень у підрозділах судових експертиз і експертних досліджень у підрозділах Експертної служби Міністерства внутрішніх справ України".

Установи, які мають право здійснювати комп'ютерно-технічну експертизу:

- Державний науково-дослідний експертно-криміналістичний центр (або його регіональні підрозділи – НДЕКЦ в областях);
- Київський науково-дослідний інститут судових експертиз;
- Львівський та Одеський науково-дослідні інститути судових експертиз Міністерства юстиції України;
- ТОВ «Лабораторія комп'ютерної криміналістики» та ТОВ "Незалежний інститут судових експертиз" у м. Київ.

*У комп'ютерно-технічній експертизі існують такі підвиди експертизи:* апаратно-комп'ютерна; програмно-комп'ютерна; інформаційно-комп'ютерна; комп'ютерно-мережна.

Завдання, що вирішуються комп'ютерно-технічною експертизою:

1. Виявлення інформації (за ключовими словами) та програмного забезпечення, що містяться на комп'ютерних носіях.
2. Відновлення видаленої інформації з носіїв інформації.
3. Дослідження відтворених комп'ютерних програм та відповідність певним параметрам (конкретним версіям чи вимогам на його розробку).
4. Виявлення ознак підключення до комп'ютерних мереж, наявності відвідування інтернет-ресурсів та історії переписки тощо.
5. Діагностичне дослідження технічних (апаратних) засобів комп'ютерної техніки, визначення функціональних можливостей та фактичного стану.

Існують вимоги до об'єктів, що надаються на дослідження в рамках КТЕ:

1. Об'єкти дослідження надаються в окремих пакуваннях, що унеможливають доступ до носіїв інформації безпосередньо, підключення системного блока до мережі живлення. Такі об'єкти дослідження, як мобільні телефони, планшетні комп'ютери, GPS-навігатори, smart-годинники портативні відеореєстратори тощо надаються в окремих непрозорих пакуваннях.
2. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду, а також технічна документація до них.
3. Об'єкти дослідження (портативні комп'ютери, відеореєстратори, планшетні комп'ютери) обов'язково надаються з блоками живлення та

паролями (кодами доступу).

4. Упакуванню підлягають усі об'єкти дослідження, які направляються на експертне дослідження. Бажано кожен об'єкт дослідження, носій з об'єктом дослідження упаковувати окремо.

Для скорочення строків виконання експертиз та підвищення доказової значущості висновку експерта доцільно здійснити коло підготовчих заходів при призначенні комп'ютерно-технічних експертиз:

- у зв'язку з великою кількістю комп'ютерного обладнання необхідно проводити попередній огляд об'єктів із залученням експертів з метою встановлення наявності даних, що можуть мати доказове значення у кримінальному провадженні і відокремлення об'єктів, які не будуть об'єктом дослідження, та з метою вирішення питання про доцільність подальшого призначення експертизи;

- обов'язково узгоджувати перелік запитань за конкретними об'єктами з фахівцями та оптимізувати кількість самих запитань. Ставити такі запитання, які стосуються безпосередньо об'єктів дослідження в конкретному кримінальному провадженні, виключаючи при цьому запитання юридичного характеру та запитання, вирішення яких не потребує спеціальних знань;

- визначати першочерговість та пріоритети дослідження наданих об'єктів;

- у разі необхідності дослідження значної кількості різноманітної комп'ютерної техніки (понад 5 одиниць жорстких дисків, системних блоків, ноутбуків тощо), рекомендується призначати окремі експертизи розмежовуючи їх за групами об'єктів дослідження;

- запитання у клопотанні слідчого не повинні носити довідковий, правовий характер і виходити за межі компетенції експерта. Запитання повинні бути спрямовані на встановлення конкретних обставин розслідуваної події.

При призначенні апаратно-комп'ютерної експертизи на розгляд експерту ставляться запитання щодо апаратного забезпечення.

При призначенні програмно-комп'ютерної експертизи ставляться запитання щодо програмного забезпечення, а при призначенні інформаційно-комп'ютерної експертизи запитання щодо інформаційного забезпечення.