



**ЕКСПЕРТНА СЛУЖБА
МВС УКРАЇНИ**

МВС УКРАЇНИ

**КИЇВСЬКИЙ НАУКОВО-ДОСЛІДНИЙ
ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР**

ІНФОРМАЦІЙНИЙ ЛИСТ

**ОСОБЛИВОСТІ ПРИЗНАЧЕННЯ ТА МОЖЛИВОСТІ СУДОВОЇ
КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ**

Київ 2023

Судова комп'ютерно-технічна експертиза – це дослідження комп'ютерної інформації, яке проводиться в процесуальній формі за дорученням органу досудового слідства чи суду з метою встановлення технічних параметрів комп'ютерної техніки; явної та видаленої інформації, що зберігається на електронних носіях; визначення функціонального призначення програмного забезпечення; дослідження мережевих технологій.

Об'єктами комп'ютерно-технічної експертизи виступають:

- системні блоки персональних комп'ютерів;
- накопичувачі на жорстких магнітних дисках;
- твердотільні накопичувачі;
- портативні персональні комп'ютери;
- планшетні персональні комп'ютери;
- флеш-накопичувачі;
- мобільні телефони;
- SIM-карти;
- відеореєстратори;
- ігрові термінали;
- Інтернет-сайти (Інтернет-сторінки);
- пластикові картки.

Орієнтовний перелік вирішуваних питань:

- Чи містяться на наданих на дослідження об'єктах серед наявних та видалених файлів інформація щодо ключових слів: «****», «***», «**» (вказати, які саме ключові слова)? Якщо так то прошу скопіювати зазначену інформацію на окремий носій.

- Чи містяться на наданих на дослідження об'єктах серед наявних та видалених файлів документи формату «doc», «docx» та електронні таблиці формату «xls», «xlsx»? Якщо так, то прошу скопіювати зазначену інформацію на окремий носій.

- Чи містяться на наданих на дослідження об'єктах файли форматів: «***», «***», «***» (вказати, які саме формати)? Якщо так то прошу скопіювати зазначену інформацію на окремий носій.

- Чи містяться на наданих на дослідження об'єктах листи електронної пошти? Якщо так то прошу скопіювати зазначену інформацію.

- На які веб-адреси мережі Інтернет та коли здійснювався вихід з наданих на дослідження об'єктів?

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

- Чи встановлені програми обміну повідомлення в мережі Інтернет «Viber», «Skype», «Telegram», «Signal», «Instagram», «Facebook Messenger»?

Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків? Прошу скопіювати дану інформацію.

- Чи містяться на наданих на дослідження об'єктах програмне забезпечення, призначене для віддаленого керування комп'ютером: «TeamViewer», «Ammyu Admin», «Radmin», «UltraVNC»? Якщо так, то прошу скопіювати лог-файли використання виявлених програм.

- Чи наявні на наданих на дослідження об'єктах програми (клієнти) дистанційного банківського обслуговування (ДБО) «Клієнт-банк», «Інтернет-банкінг»?

- Чи міститься на наданих дослідження об'єктах встановлене програмне забезпечення: «****», «****», «****» (вказати назви програмних забезпечень)? Дата та час їх інсталяції?

- Чи містяться на наданих на дослідження об'єктах (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення (у сенсі, грального бізнесу): «iConnect», «iChampion», «G-slot», «Gaminator», «Superomatic», «iGaming Casino», «Megasuperomatic»? (запропоноване питання може відноситися також і до ігрових терміналів).

- Чи містяться на наданих на дослідження об'єктах файли, які ідентифікуються антивірусним програмним забезпеченням як шкідливе програмне забезпечення?

- Чи міститься на наданих на дослідження об'єктах інформація щодо USB пристроїв, які використовувались в системі. Якщо так, то прошу зазначити їх VID, PID, серійні номери, дату та час їх підключень?

- Чи містяться на наданих на дослідження об'єктах клієнт-програми для обміну файлами через мережі P2P? Дата та час їх інсталяції? Які папки підключені до виявлених програм та чи містяться в них графічні та відеофайли? Якщо так, то чи розповсюджувались вони іншим користувачам мережі Інтернет через клієнт-програми P2P?

- Чи містяться на наданому на дослідження відеореєстраторі відеозаписи, створені (вказати дату за яку потрібні відеозаписи)? «Якщо так, то виявлені відеозаписи прошу скопіювати на окремий носій.

- Чи містяться в пам'яті наданих на дослідження об'єктів інформація щодо вмісту телефонної книги, вхідних, вихідних та не прийнятих дзвінків, текстових повідомлень, веб-історії, повідомлень в мережі Інтернет з додатків «Viber», «Skype», «Telegram», «Signal», «Instagram», «Facebook Messenger», а також файли користувача. При наявності зазначеної інформації прошу їх скопіювати на окремий носій інформації.

Експертним завданням судової комп'ютерно-технічної експертизи є:

- установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

- виявлення інформації (за ключовими словами) та програмного

забезпечення, що містяться на комп'ютерних носіях;

-установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Зазначений перелік експертних завдань не є вичерпним і може доповнюватись залежно від запиту ініціатора проведення експертного дослідження в межах компетенції комп'ютерно-технічної експертизи.

Особливості призначення судової комп'ютерно-технічної експертизи:

При призначенні комп'ютерно-технічної експертизи слідчими допускаються типові недоліки, які збільшують терміни проведення експертизи та ускладнюють або унеможливають її провадження, наприклад:

На експертизу направляються об'єкти, які не містять і не можуть містити інформацію, що має значення у кримінальному провадженні.

Однією постановою призначаються експертизи за великою кількістю об'єктів із великим об'ємом даних, при цьому не визначаючи пріоритети першочерговості.

Однією постановою призначаються експертизи за різними видами об'єктів (сервери та персональні комп'ютери або мобільні телефони та «планшетні» комп'ютери), для дослідження яких потрібно залучати відповідних спеціалістів.

На експертизу надаються об'єкти, які з певних причин фізично неможливо дослідити (відсутність елементів та кабелів живлення, відсутність відповідних програмних та апаратних засобів дослідження тощо).

З метою оптимізації навантаження на експертів за напрямом комп'ютерно-технічної експертизи та запобігання виникнення черг з призначених експертів, скорочення строків їх виконання та підвищення якісної значущості висновку експерта, як джерела доказів у кримінальному провадженні, пропонується запровадити наступний алгоритм підготовчих заходів при призначенні комп'ютерно-технічних експертів та розподілу навантаження на фахівців Експертної служби МВС України.

Перед призначенням комп'ютерно-технічної експертизи:

- проводити попередній огляд об'єктів із залученням фахівців Експертної служби МВС з метою встановлення наявності даних, що можуть мати доказове значення у кримінальному провадженні, та з метою вирішення питання про доцільність подальшого призначення експертизи;

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

- визначати першочерговість та пріоритети дослідження наданих об'єктів.

- при вилученні системні блоки та інші пристрої повинні бути відповідним чином упаковані й опечатані, щоб виключити можливість їхнього пошкодження, включення в мережу й розбирання. Використання рулонної «стретч-плівки» та липкої стрічки типу «скотч» при пакуванні і закріпленні паперових бирок з пояснювальними написами не допускається.

У разі необхідності проведення у стислі терміни дослідження значної кількості різноманітної комп'ютерної техніки (понад 10 одиниць жорстких дисків, системних блоків, ноутбуків тощо), а також при значній завантаженості відділу комп'ютерно-технічної експертизи лабораторії комп'ютерно-технічних та телекомунікаційних досліджень Київського НДЕКЦ МВС, рекомендується призначати експертизи з розмежуванням за групами об'єктів дослідження, та вирішувати питання щодо їх призначення до обласних підрозділів Експертної служби МВС або інших експертних установ Міністерства юстиції України, Служби безпеки України, у яких проводяться такі дослідження.

Київський НДЕКЦ МВС