

3. Верховный суд США разрешил обыск компьютеров в любой юрисдикции. Хабр: URL: <https://habr.com/ru/news/t/357064/> (дата звернення: 04.11.2021).

4. German federal police use Trojan virus to evade phone encryption. DW: 27.01.2018. URL: <https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466> (дата звернення: 04.11.2021).

5. German government to use Trojan spyware to monitor citizens. DW: 22.02.2016. URL: <https://www.dw.com/en/german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629> (дата звернення: 04.11.2021).

6. Кримінальний процесуальний кодекс України: Закон України від 13.04. 2012 р. № 4651-VI. Законодавство України: база даних / Верхов. Рада України. Дата оновлення: 08.08.2021. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#n1654> (дата звернення: 05.11.2021).

7. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07. 09. 2005 р. N 2824-IV. Законодавство України: база даних / Верхов. Рада України. Дата оновлення: 21.09.2010. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#n1654> (дата звернення: 05.11.2021).

Латиш Катерина Володимирівна,
асистент кафедри криміналістики
Національного юридичного університету
імені Ярослава Мудрого, кандидат
юридичних наук

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА МОБІЛЬНИХ ТЕЛЕФОНІВ: АСПЕКТИ ПРИЗНАЧЕННЯ

Під час досудового розслідування у передбаченому Кримінальним процесуальним кодексом України (далі – КПК України) порядку збираються фактичні дані, що мають значення для кримінального провадження та підлягають доказуванню. Зокрема, це дані, які містяться на телефонах та інших технічних носіях щодо встановлення наявності чи відсутності факту спілкування між сторонами кримінального процесу. Для отримання змісту цих даних слідчі призначають судові комп'ютерно-технічні експертизи та звертаються до відповідних судово-експертних установ, обґрунтовуючи це необхідністю застосування спеціальних знань. Коло об'єктів даного виду експертизи є доволі широким: комп'ютери та їх складові, будь-які носії інформації (дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (на кшталт мобільних телефонів, різноманітних гаджетів, банкоматів, гральних автоматів, принтери, сканери та ін.) [1, с. 152–153].

Найпоширенішим є проведення комп'ютерно-технічної експертизи саме мобільних телефонів, на вирішення якої можуть бути поставлені такі запитання: Який заводський номер (IMEI) мобільного телефону з присутніми картками мобільного зв'язку операторів? Які номери операторів мобільного зв'язку присвоєні сім-картам операторів мобільного зв'язку, які знаходяться у мобільному телефоні (обов'язково мають бути зазначені марка телефону, колір та IMEI)? Чи наявний у телефоні, наданому на експертизу, журнал дзвінків, текстові SMS-повідомлення та телефона книга? У разі наявності зробити з них копію або вказати назви абонентів та їх абонентські номери. Чи наявні у наданому на експертизу телефоні повідомлення, передані через програми месенджери? У разі наявності зробити з них копію. Чи наявні у наданому на експертизу телефоні у явному та видаленому стані текстові, графічні, аудіо-, відео- файли? У разі наявності зробити з них копію. Чи містяться в пам'яті наданого на дослідження мобільного телефону вебсторії, повідомлення в мережі інтернет, а також файли користувача?

Важливими є питання про надання інформації щодо даних з телефонних книг, збережених номерів у телефонах, змісту SMS повідомлень, даних GPS, які ставляться на вирішення експертам. Такі питання можуть формулюватися таким чином: «Чи містяться на наданому на дослідженні мобільному телефоні електронна переписка за допомогою програмних додатків та інтернет-месенджерів «Viber» «WhatsApp», «Telegram», «Signal», «Line», «Messenger», в тому числі видалена, за номером мобільного телефону? Якщо так, то прошу скопіювати зазначену інформацію та дані на окремий компакт-диск».

Можуть бути вказані назви інших додатків або номер конкретного абонента, з яким відбувалася переписка, та який необхідно встановити. Також слідчі можуть просити копіювання на окремий носій збережені номери в телефонах, інтернет-дані з телефонних книг, вказаних мобільних телефонів, зміст SMS повідомлень, дані GPS зі збереженими координатами.

Проте постає питання щодо правомірності таких дій щонайменше з двох причин. По-перше, такі дані відносяться до персональних, які охороняються законом. По-друге, слідчий має надати цифровий пароль або захисний код до нього, у разі, якщо слідство володіє зазначеною інформацією, для розблокування телефону чи іншого технічного носія, якого може і не бути у розпорядженні слідчого. У зв'язку з чим виникають питання, пов'язані із наданням експертам дозволу на внесення змін, у мобільний телефон, якщо він виявиться заблокованим, та наявну у ньому інформацію, які можуть призвести до зміни статусу об'єкту. Тому повинно бути вирішено питання про надання експерту дозволу на повне або часткове знищення мобільного телефону або зміну його властивостей. Однак, такі дії можна кваліфікувати, як подолання системи «логічного захисту», на що потрібна окрема ухвала слідчого судді.

Разом з тим, вбачаються проблеми з копіюванням на окремий носій інтернет-даних з телефонних книг, вказаних мобільних телефонів, у тому числі даних про збережені номери в телефонах, зміст SMS повідомлень, дані GPS зі збереженими координатами. Це обумовлено тим, що такі дані відповідно до п. 7 та п. 8 ч. 1 ст. 162 КПК України відносяться до охоронюваної законом таємниці і процесуальний порядок отримання таких даних визначений у главі 15 розділу II КПК України. Під час судового провадження такий порядок регулюється ч. 2 ст. 333 КПК України шляхом надання тимчасового доступу до речей і документів.

Також зустрічаються випадки проведення огляду мобільних телефонів у порядку статті 237 КПК України, у ході якого слідчі за участі спеціалістів за допомогою апаратного комплексу UFED Touch 2 знімають інформацію із вказаних мобільних телефонів: телефонної книжки із переліком збережених телефонів, телефонних з'єднань, у тому числі SMS, MMS з датою та тривалістю дзвінків із зазначенням абонентів.

Однак, з такими діями не можна погодитися, оскільки положення ст. 237 КПК України визначають порядок проведення огляду та встановлюють дії які можуть бути проведені в ході нього. Але зняття інформації із вказаних мобільних телефонів не може бути проведено в ході такої слідчої дії, як огляд. Зняття інформації із вказаних мобільних телефонів: телефонної книжки із переліком збережених телефонів, телефонних з'єднань, в тому числі SMS, MMS з датою та тривалістю дзвінків із зазначенням абонентів, не охоплюється визначеним вказаною статтею діями. Натомість, КПК України передбачає спеціальний порядок отримання такої інформації, зокрема який передбачений ст. 264 КПК України. Зняття інформації з електронних інформаційних систем регулюється главою 21 КПК України, яка визначає порядок проведення негласних слідчих (розшукових) дій [2].

Крім того, трапляються випадки, коли слідчий вдається до зайвої деталізації при постановці запитань експертів або ставить питання, які виходять за межі його компетенції, або такі, відповіді на які слідчий вже самостійно надав шляхом огляду речей та вказав це у відповідних протоколах та постановках. Наприклад, такі питання: «Чи обладнані мобільні телефони (зазначення марки, кольору, IMEI) картками мобільних операторів? Які номери телефонів присвоєні сім-карткам операторів мобільного зв'язку, які знаходяться у вказаних мобільних телефонах?». Разом з тим, у постанові про визнання речовими доказами вже було вказано сім-картками яких операторів обладнані ці мобільні телефони та їх абонентські номери.

Таким чином, важливим є врахування вищезазначених питань при призначенні судової комп'ютерно-технічної експертизи, оскільки здійснення процесуальних дій, які потребують попереднього дозволу суду, без такого дозволу або з порушенням його суттєвих умов, є істотним порушенням прав людини та основоположних свобод [3].

Список використаних джерел

1. Грига М. А. Аспекти проведення експертиз під час розслідування кіберзлочинів // Актуальні питання криміналістики та судової експертизи: матеріали Всеукр. наук.-практ. конф. (Київ, 19 листоп. 2020 р.) / [редкол.: В. В. Черней, С. Д. Гусарев, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2020. – С. 151-154.
2. Ухвала Кам'янка-Бузького районного суду Львівської області від 03 квітня 2019р. по справі №446/1117/16-к.
3. Ухвала ВССУ від 12.11.2015р. у справі №5-2095км15.

Леонтюк Юлія Вікторівна,
засновниця інтернет платформи «Юридична
терапія»

СТАН ЦИФРОВОЇ ЗАЛЕЖНОСТІ ЯК ОBOB'ЯЗKOBA ХАРАКТЕРИСТИКА ПОТЕРПЛОГО ТА СУБ'ЄКТА ЗЛОЧИНУ В НАЙБЛИЖЧОМУ МАЙБУТНЬОМУ

«Nothing vast enters the life or mortals
without a curse» Sophocles/ Епіграф до
фільму «Соціальна дилема»

Кримінальний кодекс України (далі – КК України) і Міжнародний класифікатор хвороб (далі – МКХ) регулюють різні сфери життя людини і призначені для різних суб'єктів застосування, однак у своїй основі мають однакову функцію – кваліфікація проблеми медичного чи кримінального характеру та діючі шляхи до її вирішення. Враховуючи той факт, що прийнятий МКХ-11 в травні 2019 року, буде введений в дію на початку 2022 року, вважаємо за необхідне розібратись в його нововведеннях і тих позиціях, які в цей документ не ввійшли, але навколо яких точилась запекла дискусія.

Основні зміни МКХ 11 стосуються наступних позицій:

- Уточненні специфічні симптоми ПТСР;
- Альтернативна медицина визнана як норма;
- Ігрова залежність онлайн і офлайн тепер є психічним захворюванням;
- Інсульт тепер є хворобою мозку, а не системи кровообігу;
- Категорія психічних розладів ЛГБТ перейшли в категорію психічного здоров'я.

На етапі обговорень МКХ -11 піднімалися питання руйнівного впливу на психіку гаджетів та введення таких діагнозів: цифрова залежність, цифрове недоумство та інформаційна псевдодибільність, однак, посилаючись на недостатність емпіричних даних нейробіологів, які більшою мірою посилались на свою діагностику і МРТ дослідження, які фіксують результат, подібно поліграфу, може зафіксувати зміни в мозку, але він не зафіксує на що були ці зміни. А вихід в 2020 році фільму «Соціальна дилема» на Netflix, тільки