Перелік джерел посилання

1. Про реалізацію експериментального проєкту щодо використання віддаленого кваліфікованого електронного підпису: постан. Кабміну України від 02.09.2020 р. № 785. URL: https://zakon.rada.gov.ua/laws/show/785-2020-п#Text (дата звернення: 10.09.2023).
2. Пріоритетні напрями та завдання (проєкти) цифрової трансформації на період до 2023 року: розпорядж. Кабміну України від 17.02.2021 р. № 365. URL: https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#Text (дата звернення: 10.09.2023).
3. Rasa Tamošiūnaitė. Handwriting expertise in the forensic science centre of Lithuania: present actions and future vision. *Криміналістика і судова експертиза*. 2022. № 67. С. 365—371.
4. 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 Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.09.2023).
5. Золота Л. В., Савченко І. О. Проблематика призначення почеркознавчої експертизи в цивільному судочинстві. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. № 70. С. 175—180.

Інформація стосовно активності користувача в операційній системі *Windows* як джерело доказів під час досудового розслідування

Євгеній Тарасенко,
Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: t.expert.kte.sumy@gmail.com

Розглянуто актуальність дослідження активності користувача в операційній системі Windows та можливість використання цих даних під час досудового розслідування.

***Ключові слова**: операційна система; користувач; журнал подій; досудове розслідування.*

Windows Operational System User's Activity as Evidence Source During Pre-Trial Investigation

Evgeniy Tarasenko

This article explores relevance to examine the Windows OS user's activity and whether this data applicable for pre-trial investigation.

***Keywords**: operational system; user; event log; pre-trial investigation.*

У сучасних кримінальних провадженнях доволі часто згадується комп'ютерна техніка, яка в процесі досудового розслідування досліджується на предмет різної інформації, яка може мати значення для слідства. З-поміж таких даних є інформація стосовно активності користувача, що вказує на те, які саме дії виконував користувач на комп'ютері та в який час. Під час розслідування можна порівняти ці журнали з показаннями фірурантів тієї чи тієї справи та визначити правдивість їх показань.

В операційній системі *Windows* зберігається чимало журналів активності, які допоможуть визначити, які саме дії виконував користувач та в який час. Нижче наведено основні типи журналів та яка інформація в них зберігається.

Системні журнали. У цій категорії зберігають інформація про системні події: завантаження системи, установлення та видалення програмного забезпечення, установлення служб та драйверів, обладнання, підключені пристрої та інші системні події. Також в цій категорії зберігається інформація про останні відкриті файли та каталоги, а також запущені програми.

Журнали безпеки. У цих журналах зберігають інформація про події, пов'язані з безпекою системи: спроби входу, зміни прав доступу, записи антивірусного програмного забезпечення та інші дії, які можуть вплинути на безпеку системи.

Журнали програмного забезпечення. У цій категорії зберігають інформація про роботу інстальованого програмного забезпечення. Тут може зберігатися інформація про запуск програмного забезпечення, налаштування та помилки, які виникли під час його роботи. Тип інформації, яка може зберігатися в таких журналах, відрізняється в залежності від програмного забезпечення та його налаштувань.

Під час аналізу журналів подій та активності користувача перше, на що варто звернути увагу, це дата та час входу в систему. Не менш важливою є інформація про останні дії користувача: відкриті файли чи програмне забезпечення, яке було запущено в певний час. Інформація про підключені пристрої стане в пригоді, якщо потрібно встановити, чи підключався, наприклад, той чи той флеш-накопичувач до комп'ютера. Інформація про роботу інстальованого програмного забезпечення може мати значення в залежності від його типу. Наприклад, якщо це програмне забезпечення призначене для віддаленого доступу, у його журналах може зберігатися інформація про дату та час таких підключень та, за можливості, інші дані: назва віддаленого комп'ютера або його ір-адреса. До активності користувача також може належати інтернет-історія браузера (програма для доступу до інтернет-ресурсів). У журналі браузера зберігається інформація про те, на який сайт було здійснено доступ та в який час, також можна виявити інформацію про пошукові запити, які вводив користувач. Важливо враховувати, що обсяг та тривалість зберігання журналів активності можуть бути обмеженими і залежати від налаштувань системи, а також від того, чи була увімкнена функція «журналювання» Користувач може також чистити (видаляти) історію своєї активності.

Проаналізувавши інформацію про активність користувача в операційній системі Windows, її можна порівняти з показаннями особи та визначити правдивість її тверджень під час допиту, наприклад, коли особа вказує, що вона не працювала в цей час за комп'ютером чи не заходила на певні інтернет-ресурси, або не вчиняла інші дії, які були виявлені під час аналізу активності користувача. Такий метод розслідування допомагає виявити неправдиві свідчення та визначити, де саме є розходження з виявленою інформацією та показаннями, які дає особа.

Перелік джерел посилання

1. Russinovich M., Solomon D., Ionescu A.. Windows Internals: System architecture, processes, threads, memory management, and more. 2020 year. 800 ст.
2. Windows Event log веб-сайт. URL: https://learn.microsoft.com/en-us/windows/win32/wes/windows-event-log (дата звернення: 28.08.2023).
3. Windows activity history and your privacy веб-сайт. URL: https://support.microsoft.com/en-us/windows/-windows-activity-history-and-your-privacy-2b279964-44ec-8c2f-e0c2-6779b07d2cbd (дата звернення: 28.08.2023).

Використання безпілотного літального апарата (дрона) під час розслідування кримінальних правопорушень

Дмитро Тичина,
канд. юрид. наук, Національна академія внутрішніх справ, м. Київ, Україна,
ORCID: https://orcid.org/0000-0002-9430-6101, e-mail: ddt0099@gmail.com
Роман Перцев,
д-р філос. з галузі права, Центральний округ поліції Ізраїлю, м. Рамля, Ізраїль,
ORCID: https://orcid.org/0000-0001-9471-2962, e-mail: romanpertsev82@gmail.com

Діяльність слідчого на початковому етапі досудового розслідування є єдиною, взаємозалежною системою процесуальних дій, спрямованих на виявлення, фіксування, вилучення та дослідження слідів кримінального правопорушення, визначаючи подальшу спрямованість наступного етапу розслідування. Розслідування кримінальних правопорушень потребує сучасних, новітніх, практичних засобів на основі проведених комплексних науково-праксеологічних досліджень із використанням цифрових технологій під час проведення слідчих (розшукових) дій. Практичне використання