

Засоби збереження первинного стану об'єктів при дослідженнях на цифрових носіях

Олег Литвицький

завідувач сектору, Запорізький НДЕКЦ МВС України, м. Запоріжжя, Україна,
e-mail: litvicki@ukr.net

Олена Литвицька

головна судова експертка, Запорізький НДЕКЦ МВС України,
м. Запоріжжя, Україна, e-mail: alena.litvitskaya@gmail.com

Розглянуто засоби, які можуть бути використані при дослідженнях об'єктів, наданих на цифрових носіях, для збереження їх первинного стану.

Ключові слова: цифрові носії; інформація; первинний стан; захист.

Means of Preserving the Original State of Objects in Digital Media Research

Oleh Lytvytskyi, Olena Lytvytska

The paper outlines means that can be employed in the research on objects provided on digital media to preserve their original state.

Keywords: digital media; information; original state; protection.

Сьогодні існує багато напрямів судової експертизи, і деякі з них передбачають дослідження об'єкти, що містяться на цифрових носіях, зокрема, фототехнічні, портретні, комп'ютерно-технічні експертизи тощо.

Відповідно до ст. 5 Закону України «Про судову експертизу» «Під час проведення судових експертиз (обстежень і досліджень) об'єкти дослідження можуть бути пошкоджені або витрачені лише у тій мірі, в якій це необхідно для дослідження» [1], а під час дослідження цифрових носіїв відбувається взаємодія з комп'ютерною технікою, отже неминуче відбувається вплив на первинний стан наданого носія.

Тому актуальним є питання збереження інформаційного наповнення в первинному стані, тобто виключення можливості видалення або запису будь-яких даних на досліджуваний носій.

Найбільш розповсюдженими є такі типи носіїв:

- жорсткі диски (HDD) та твердотільні накопичувачі (SSD);
- оптичні диски (CD, DVD, Blu-ray);

- USB-флеш накопичувачі;
- різноманітні карти пам'яті (SD, micro-SD тощо).

Кожен із зазначених пристроїв має свої принципи та технологію запису і зберігання інформації, отже, залежно від типу носія доступ до інформаційного наповнення здійснюється за допомогою різних технічних засобів.

Незалежно від типу носія забезпечити збереження його первинного стану можна двома способами — програмним та апаратним.

Апаратний спосіб передбачає використання спеціалізованого обладнання, яке блокує запис або видалення даних із носія.

Програмний спосіб впливає на налаштування операційної системи, що, як і при апаратному способі, блокує запис або видалення даних із носія.

Розглянемо їх більш докладно.

Доступ до інформації, яка міститься на жорстких дисках, картах пам'яті та USB-флеш накопичувачах здійснюється через спеціальний інтерфейс (найчастіше, USB-

сумісні перехідники або просто USB-інтерфейс), тому доцільно використовувати пристрої блокування запису.

Зараз існує доволі багато пристроїв такого класу, в Україні найбільш розповсюдженим є пристрій серії «Tableau Forensic», який дає змогу здійснювати доступ до даних на досліджуваному накопичувачі інформації, не вносячи до нього будь-яких змін [2].

Якщо немає можливості скористатись засобами апаратного блокування, існує низка спеціалізованих програмних засобів, які дають змогу контролювати доступ до USB-портів робочої станції експерта: до них належать спеціалізоване програмне забезпечення, наприклад, USB Write Protector, NetSoftwares USB Block [3], ncfs, а також базові утиліти, наявні в операційній системі, наприклад для «Windows» — «Diskpart» [4], яка дає змогу встановити статус для накопичувачів «Тільки для читання».

Реалізація зберігання інформації на оптичних дисках базується на фізичній зміні його структури й не передбачає змін під час доступу до його інформаційного наповнення, але не виключає можливих технічних збоїв, тож під час дослідження даного типу носіїв доцільно використовувати пристрої,

передбачені тільки для читання, що дасть змогу уникнути можливості пошкодити дані на носії, а також захистити його в первинному стані.

Отже, сьогодні існує велика кількість різновидів носіїв інформації, які відрізняються за своєю будовою та принципами організації запису та зберігання даних, тому наявні різноманітні засоби захисту їх інформаційного наповнення.

Перелік джерел посилання

1. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/4038-12#Text> (дата звернення: 14.09.2023).
2. Пристрої блокування запису та дублювання даних. URL: <https://cybermarket.com.ua/product-category/write-blockers/> (дата звернення: 14.09.2024).
3. Restrict Access of Portable Drives. URL: <https://www.newsoftwares.net/usb-block/> (дата звернення: 14.09.2024).
4. Microsoft Ignite. URL: <https://learn.microsoft.com/windows-server/administration/windows-commands/diskpart> (дата звернення 14.09.2024).