Методичні аспекти комплексного дослідження технічних засобів на базі одноплатних мінікомп'ютерів

Ігор Настопиров
головний судовий експерт, Український науково-дослідний інститут спеціальної техніки
та судових експертиз Служби безпеки України, м. Київ, Україна,
ORCID: https://orcid.org/0009-0006-6434-6774, e-mail: igadomino@gmail.com

Розглянуто методичні аспекти експертизи одноплатних мінікомп'ютерів як спеціальних технічних засобів негласного отримання інформації. Запропоновано підхід, що містить аналіз даних, конструкції та експеримент.

Ключові слова: *одноплатні мінікомп'ютери; судова експертиза; спеціальні технічні засоби негласного отримання інформації; експертний експеримент.*

Methodological Aspects for Comprehensive Study of Technical Devices Powered by Single-Board Microcomputers

Ihor Nastopyrov

This paper addresses methodological aspects pertaining to forensic examination of single-board microcomputers as specialised technical devices for covert information gathering. An approach is proposed combining data analysis, design, and experimentation.

Keywords: *single-board microcomputers; forensic examination; specialised technical devices for covert information gathering; expert experimentation.*

Одноплатні мінікомп'ютери є універсальними обчислювальними пристроями; що функціонують під керуванням повноцінних операційних систем. Завдяки компактним розмірам, низькому енергоспоживанню та наявності вбудованих мережевих інтерфейсів їх широко застосовують як апаратну платформу для різноманітних технічних засобів, зокрема спеціальних технічних засобів негласного отримання інформації (далі — *СТЗ НОІ*), включно з прихованим записом і передаванням аудіоінформації [1].

Зазвичай такі мінікомп'ютери надходять на експертне дослідження у складі конструкцій, замаскованих під побутові або інші предмети, а також у саморобних корпусах, оскільки самі вони є друкованою платою з електронними компонентами.

Основна проблематика експертного дослідження полягає у складності встановлення фактичного функційного призначення технічного засобу загалом, оцінюванні його технічної придатності для негласного отримання інформації. Це зумовлено високою гнучкістю конфігурації програмного забезпечення та інтеграцією пристрою в камуфльовані конструкції. Зазначені особливості зумовлюють необхідність застосування комплексного підходу, який поєднує аналіз інформаційного наповнення носіїв даних, дослідження конструктивних особливостей пристрою та проведення експертного експерименту. Такий підхід дає змогу обґрунтовано дати відповідь на питання про належність чи неналежність досліджуваного об'єкта до СТЗ НОІ.

Важливим початковим етапом є аналіз інформаційного наповнення носіїв даних мінікомп'ютера. Дані можуть зберігатися як на вбудованих накопичувачах типу *eMMC*, так і на знімних носіях (*microSD*-картках). Дослідження *microSD*-карток проводять із застосуванням криміналістичних програмних засобів з обов'язковим створенням *bitwise*-копії носія. Доступ до вбудованої пам'яті *eMMC* зазвичай забезпечують завантаженням пристрою з підготовленого зовнішнього носія з *Linux*-сумісною операційною системою з контролем процесу через інтерфейс *UART*. Після отримання доступу виконують копіювання даних для подальшого аналізу.

Комплексне дослідження носіїв дає змогу виявити програмні компоненти, призначені для запису аудіоінформації, установити наявність файлів аудіозаписів, а також з'ясувати механізми їх зберігання та передавання. У процесі аналізу часто виявляють такі

програмні засоби, як *ALSA* та *SoX* (для запису аудіо), *DarkIce*, *IceS*, *edcast* (для потокового передавання), *Icecast2* та *SHOUTcast* (для транслювання), *TeamSpeak*, *OBS* (для передавання аудіо). Окремо вивчають наявність мережевих компонентів (*NetworkManager*, *OpenVPN* тощо), які можуть забезпечувати передавання інформації, зокрема, через захищені канали.

Під час дослідження конструкції експерт оцінює характер і якість камуфлювання, спосіб розміщення елементів системи, наявність ознак прихованого функціювання, особливості розташування мікрофонів та акустичних каналів, а також методи маскування світлової індикації роботи пристрою.

Визначальним етапом є експертний експеримент, який дає змогу підтвердити або спростувати реальну реалізацію виявлених технічних можливостей. У процесі експерименту перевіряють можливість запису аудіоінформації, якість і параметри запису, умови його ініціації (автоматичний запуск, запуск за подією тощо). Досліджують також здатність пристрою передавати аудіоінформацію різними каналами зв'язку, можливість дистанційного керування (підключення за допомогою мережі, запуск / зупинка запису, зміна параметрів).

Сукупність ознак, установлених під час експерименту, дає підстави для обґрунтованого висновку щодо фактичної працездатності пристрою як засобу отримання аудіоінформації.

За результатами комплексного дослідження встановлюють два основні аспекти: придатність (технічна можливість виконувати функції запису, зберігання та передавання аудіоінформації) і призначеність (спрямованість конструктивного, програмного та функційного рішення на негласне отримання інформації) [2]. Наявність спеціалізованих програмних засобів свідчить про технічну забезпеченість відповідних функцій, тоді як ознаки прихованого виконання та камуфлювання — про орієнтування на негласне застосування. Рішення про належність досліджуваного пристрою до СТЗ НОІ експерт приймає за сукупністю всіх визначених ознак з урахуванням не лише технічних характеристик, а й результатів функціювання в характерних умовах застосування, програмного наповнення, конструктивних особливостей і способу маскування.

Отже, запропонований підхід до комплексного багатокритеріального оцінювання показників дає змогу обґрунтовано визначати належність або неналежність об'єктів дослідження до СТЗ НОІ. Наведені аспекти застосування багатокритеріального оцінювання результатів дослідження технічних засобів на базі одноплатних мінікомп'ютерів як засобів негласного отримання інформації можуть бути впроваджені в судово-експертну практику та сприятимуть удосконаленню методичного забезпечення дослідження технічних засобів, створених на їх основі.

Перелік джерел посилання

1. Sjogelid S. Raspberry Pi for Secret Agents. 2nd ed. Birmingham : Packt Publishing, 2015. 206 p.
2. Експертиза спеціальних технічних засобів негласного отримання інформації : заг. метод. / Укр. НДІ спецтехніки та судекспертиз СБУ. Київ, 2021 // Реєстр методик проведення судових експертиз : вебсайт. Реєстр. код 17.0.05 від 28.01.2022. URL: https://rmpse.minjust.gov.ua/search (дата звернення: 12.04.2026).