Дослідження *Raspberry Pi* як складової ворожих БпЛА

Станіслав Тульвінський
судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень,
Черкаський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України, м. Черкаси, Україна,
ORCID: https://orcid.org/0000-0001-8065-7659; email: tulvinskyi@ndekc.ck.ua

Здійснено аналіз застосування Raspberry Pi у ворожих БпЛА з акцентом на судово-експертне дослідження енергонезалежної пам'яті (microSD/eMMC), файлової системи Raspbian, мультимедіа та мережевих кінцевих точок для судової практики.

Ключові слова: *Raspberry Pi; БпЛА; судова експертиза.*

Forensic Examination of Raspberry Pi as a Component of Hostile UAVs

Stanislav Tulvinskyi

The report analyzes the use of Raspberry Pi in hostile UAVs, with emphasis on forensic examination of non-volatile memory (microSD/eMMC), the Raspbian file system, multimedia, and network endpoints for forensic practice.

Keywords: *Raspberry Pi; UAVs (Unmanned Aerial Vehicles); forensic examination.*

Із початку повномасштабного вторгнення російської федерації на територію суверенної України як озброєння використовують не лише товари подвійного призначення, а й повністю цивільні технології. Яскравим прикладом є мікрокомп'ютер *Raspberry Pi*, який ворог почав активно використовувати в конструкціях безпілотних літальних апаратів. На етапі першого масового використання ударних БпЛА типу *Shahed-136* випадків використання *Raspberry Pi* у складі конструкції не зафіксовано, проте згодом, ймовірно, з метою розширення функціональних можливостей озброєння, противник почав комплектувати ударні апарати мікрокомп'ютерами *Raspberry Pi*, додатково оснащеними периферією — мобільними модемами, веб-камерами та іншими інтерфейсними модулями. Наявність таких елементів формує новий масив об'єктів, які підлягають судово-технічному дослідженню в межах криміналістичної практики [1].

Основну увагу судового експерта під час дослідження *Raspberry Pi* як складової частини ворожого БпЛА зосереджено на енергонезалежній пам'яті мікрокомп'ютера, що переважно реалізована у вигляді *microSD*-картки або зовнішнього накопичувача; у деяких варіантах конструкції, зокрема *Compute Module*, енергонезалежна пам'ять представлена вбудованим *eMMC*. Типова ОС — *Raspbian* (нині *Debian-based* дистрибутиви), яка визначає структуру розділів: завантажувальний *FAT*-розділ з файлами прошивки та конфігураціями завантаження й кореневу файлову систему *ext4* з логами, конфігураціями користувачів, профілями мережі та прикладним програмним

забезпеченням. Судовий експерт повинен фіксувати стан фізичного носія та компонування пристрою до початку роботи з ним, забезпечити ланцюг збереження доказів та здійснити кваліфіковане вилучення пам'яті із застосуванням апаратних або програмних засобів, які гарантують відсутність модифікації даних та забезпечують обчислення контрольних сум *(SHA-256, MD5)* для подальшого підтвердження цілісності образів.

Під час вилучення та створення образів енергонезалежної пам'яті судовий експерт застосовує методи побітового копіювання з урахуванням особливостей файлової системи та можливих механізмів логічного та фізичного облаштування пристрою. Для *microSD*-карт рекомендовано застосовувати апаратні дублікатори з функцією блокування запису або програмні інструменти в поєднанні з апаратними адаптерами-блокувальниками. Після отримання бітової копії судовий експерт проводить первинний аналіз файлової системи, ідентифікацію розділів, відновлення таблиць розділів та відновлення видалених файлів з урахуванням особливостей поведінки *Linux*-файлових систем та можливих механізмів журналювання [2].

Артефакти, які мають практичну значимість у судово-експертній практиці, містять системні журнали *(systemd-journal, /var/log/)*, файли конфігурації мережевих інтерфейсів та модемів (*wpa_supplicant.conf, /etc/network/interfaces*, конфігурації *ppp* та *qmi*), збережені облікові записи та ключі доступу (наприклад, *SSH*-ключі в */home/.ssh*), історії shell-команд, плани запуску *(cron, systemd timers)*, а також скрипти автозавантаження та спеціалізоване програмне забезпечення для управління камерою або модемом. Окрему увагу слід звернути на наявність мультимедійних файлів — фотографій та відеозаписів, їхні метадані *(EXIF)*, часові позначки та, за наявності, геоприв'язки. Часто застосовують автоматизовані засоби захоплення зображень, результати роботи яких зберігаються у відомих директоріях або передаються на віддалені кінцеві точки за допомогою *HTTP POST, FTP, MQTT* або через мобільні канали зв'язку. Конфігураційні файли цих утиліт можуть містити адреси серверів, облікові дані та параметри передачі.

Аналіз мережевих компонентів периферії є невід'ємною складовою судово-експертного дослідження, адже модеми, *SIM*-модулі та *USB-GPRS/3G/4G*-модулі можуть мати інформацію про *IMEI/IMEISV*, *IP*-адреси мобільного оператора, налаштування *APN*, а також містити повідомлення та логи передачі даних. Судовий експерт під час дослідження повинен відтворити логіку взаємодії мікрокомп'ютера з модемом, установити наявність скриптів автоматичної передачі даних та зафіксувати кінцеві адреси, на які спрямовувалися медіафайли або телеметрія. Якщо пристрій використовує веб-камеру, у файловій системі можуть бути знайдені тимчасові файли, буфери відео та записи, які дають змогу встановити часові межі фіксування ЦА та напрямки спостереження.

Для ефективного судово-експертного дослідження важливо застосовувати методи відновлення інформації з неприпиненої та неповної файлової системи, аналізу незадіяного простору та пошуку слідів модифікації прошивки або бутлоадера [3]. Застосування інструментів для аналізу образів, таких як *The Sleuth Kit, Autopsy, binwalk* для виявлення вбудованих прошивок, *exiftool* — для метаданих, *bulk_extractor* — для витягання мережевих артефактів і спеціалізованих утиліт для роботи з *SQLite*-базами даних, дає змогу відтворити ланцюжок дій пристрою. Судовий експерт також має враховувати можливість прихованих механізмів передачі через стеганографію, шифровані контейнерні сховища або використання зовнішніх модулів пам'яті, доступ до яких може потребувати додаткових процедур технічного вилучення.

Практичні аспекти судово-експертної практики передбачають документування кожного етапу операцій з доказами, формування повного та обґрунтованого технічного висновку з посиланням на методики виконаних дій, хеш-значення доказів та опис виявлених артефактів, які мають значення для процесуального розгляду. Особливу увагу слід приділяти кореляції часових позначок у файлах із реальними часовими подіями, синхронізації часових зон та перевірці можливих маніпуляцій із системним часом. Судовий експерт зобов'язаний окремо зазначити джерела невизначеності або обмеження проведеного дослідження, зокрема пошкодження носія, застосування шифрування або відсутність логів.

Війна спричинила суттєві корективи не лише в цивільному житті, а й у напрямах криміналістичних досліджень, зумовивши появу нових типових об'єктів експертиз та модифікацію методик. Значущість дослідження енергонезалежної пам'яті *Raspberry Pi* як елементу ворожого озброєння обумовлена як можливістю отримання прямої технічної інформації про функціональне призначення пристрою, так і здатністю виявити сліди комунікацій із зовнішніми кінцевими точками, носії мультимедіа, конфігурації управління та засоби дистанційного контролю. Судовий експерт, застосовуючи відповідні методики вилучення, збереження та аналізу цифрових доказів, забезпечує отримання релевантних даних для судової практики та формування надійних техніко-криміналістичних висновків.

Перелік джерел посилання

1. Гончарук Г. М. Запровадження та становлення судової експертизи безпілотних літальних апаратів. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки.* 2021. № 2 (71). С. 70—75. DOI: 10.32838/TNU-2707-0581/2021.2/012 (дата звернення: 12.09.2025).
2. Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Львівського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2023. Вип. 2 (102). С. 289—305. DOI: 10.33766/2524-0323.102.289-305 (дата звернення: 12.09.2025).
3. Горішній Є. І., Волоков В. О., Струк І. А. Безпілотні літальні апарати, їх класифікація та використання. *Криміналістика та судова експертиза у XXI столітті* : матли всеукр. наук.-практ. семінару. (Київ, 30.05.2024). Київ, 2024. 291 с. URL: https://ndekc.lviv.ua/pdf/18.06.2024.pdf (дата звернення: 12.09.2025).