УДК 004.414.3:004.056

Палагін В.В., д.т.н., професор
Гончаров А.В., к.т.н., професор
Пташкін Р.Л., викладач
Черкаський державний технологічний університет
Черкаський науково-дослідний експертно-криміналістичний центр
МВС України

МЕТОДОЛОГІЯ АПАРАТНОГО РЕЇНЖИНІРИНГУ ТА КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ОБЧИСЛЮВАЛЬНИХ ПЛАТФОРМ

В умовах сучасної збройної агресії ударні безпілотні літальні апарати (БПЛА) перетворилися на складні мультипроцесорні системи, що постійно модернізуються. Необхідність апаратного реїнжинірингу (hardware reverse engineering) зумовлена потребою ідентифікації реального функціонального призначення кожного модуля, виявлення походження компонентної бази та розуміння алгоритмів керування. Криміналістичне дослідження електронної «начинки» дозволяє не лише встановити тактико-технічні характеристики апарату, а й отримати цифрові докази щодо каналів постачання складників та методів програмування польотних завдань.

Головна проблема дослідження полягає у високій варіативності та динамічній еволюції компонентної бази: постійно адаптується архітектура, переходячи від спеціалізованих сигнальних процесорів (наприклад, серії TMS320) до загальнодоступних мікроконтролерів (як-от STM32), що потребує постійного оновлення бібліотек сигнатур. Відсутність традиційних «чорних скриньок» унеможливлює стандартне зчитування логів, змушуючи експертів вдаватися до складних методів chip-off або використання інтерфейсів налагодження JTAG/SWD.

Основними інструментами для вирішення цих викликів сьогодні є:

- апаратні аналізатори - використання логічних аналізаторів для реверс-інжинірингу протоколів обміну даними;
- програмні середовища дисасемблювання - застосування інструментів для статичного аналізу бінарного коду прошивок з метою виявлення прихованих функцій передачі телеметрії;
- інструменти неруйнівного контролю - рентгеноскопія багатошарових друкованих плат для відновлення топології з'єднань, що прихована під компонентами в корпусах BGA.

Додатковим викликом є аналіз «цивільних» надбудов на базі Raspberry Pi, де криміналістичне дослідження зміщується у площину

аналізу файлових систем Linux та деконструкції скриптів на Python, що керують модемами зв'язку. Це створює ситуацію, де класична експертиза має поєднуватися з методами Live Forensics для реконструкції мережевої активності БПЛА.

Запропонований метод дослідження базується на комплексній методології ієрархічного реверс-інжинірингу, що розглядає БПЛА не як цілісний об'єкт, а як розподілену мультипроцесорну екосистему. Ключова увага приділяється деконструкції модульного стека центральної обчислювальної системи, побудованої на сімействі процесорів TMS320, та аналізу розподіленого навігаційного комплексу на базі STM32. Такий аналіз дозволяє виявити логіку паралельної обробки сигналів і механізми забезпечення живучості апарату, що є критично важливим для розробки ефективних алгоритмів протидії на рівні фізичного керування польотом.

Особливе значення має ізоляція та прикладне дослідження автономної комунікаційної надбудови на базі Raspberry Pi під керуванням ОС Raspbian. Оскільки цей вузол функціонує як закритий інтелектуальний шлюз для збору розвідувальної інформації через комерційні мережі 3G/4G та Wi-Fi, метод фокусується на детекції прихованих каналів передачі даних у месенджери та хмарні сервіси. Виявлення алгоритмів роботи «цифрової надбудови» дозволяє реконструювати сценарії використання БПЛА як активного розвідувального модуля, що ідентифікує райони роботи засобів РЕБ та здійснює фотофіксацію об’єктів у реальному часі.

Таким чином, застосування методології апаратного реїнжинірингу дозволяє оперативно адаптувати засоби РЕБ та ППО до нових модифікацій озброєння та проактивного розуміння технологічного циклу оновлення БПЛА, що підвищує ефективність захисту об’єктів критичної інфраструктури та створює доказову базу для документування.

Список використаних джерел

1. Серії «ЫІ» та «Ъ» — як росія модернізує «шахеди» та інші ударні БПЛА / Головне управління розвідки Міністерства оборони України. 2025. 18 лют. URL: https://gur.gov.ua/content/serii-y-ta-iak-rosiia-modernizuie-shakhedy-ta-inshi-udarni-bpla.html.

2. Романюк Д. Аналіз БПЛА-камікадзе противника, відмінності компонентів, додаткове обладнання. Інформаційна безпека та системи протидії (ISPS-2025) : зб. тез Міжнар. наук.-практ. семінару (м. Київ, 2025 р.). URL: https://crsi.mil.gov.ua/files/isps/isps-collection-2025.pdf.