# ВПЛИВ ТЕХНОЛОГІЇ ПОВНОГО ШИФРУВАННЯ ДИСКА НА МЕТОДИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Алфьоров С.П.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: serhii.alforov@nure.ua

**Abstract**

*The paper provides an analytical overview of how Full Disk Encryption (FDE) technologies transform digital forensic methodologies. Based on recent research on hardware-assisted key recovery, lawful access frameworks and side-channel approaches, the study compares their efficiency, limitations and legal context. Conclusions highlight the adaptive response of digital forensics to encryption-driven challenges and propose general recommendations for maintaining forensic effectiveness in an era of pervasive FDE.*

Сучасна цифрова інфраструктура все частіше ґрунтується на використанні технологій повного шифрування диска (Full Disk Encryption, FDE). Інтеграція таких систем, як BitLocker, LUKS чи FileVault, підвищує рівень захисту інформації, але ускладнює роботу фахівців цифрової криміналістики. Якщо раніше експерт міг отримати доступ до даних шляхом зчитування образу носія, то тепер більшість вмісту зберігається у зашифрованому вигляді, а ключі шифрування часто прив'язані до апаратних модулів TPM або захищених середовищ виконання. Це змінює саму логіку збору доказів – від статичного аналізу диска до динамічного аналізу процесів, пам'яті та взаємодії програмних і апаратних компонентів.

Технічні підходи до отримання доступу до зашифрованого вмісту сьогодні охоплюють декілька взаємодоповнюючих напрямків. Перший напрямок пов'язаний із «живим» зняттям пам'яті: збирання дампу оперативної пам'яті та системного контексту в момент, коли том розблоковано, дозволяє знайти похідні ключові матеріали або самі ключі у вигляді байтових структур [1]. Другий напрямок пов'язаний із апаратними інтервенціями через інтерфейси налагодження і прямого доступу до пам'яті (наприклад, інструменти, що використовують DCI/DMA), які у певних конфігураціях дають змогу отримати Volume Master Key без розкриття паролю [2]. Третій напрямок – застосування сайд-канальних методик, зокрема електромагнітного аналізу, що дозволяє реконструювати криптографічні операції та зменшити простір пошуку ключів [1]. Кожен із цих підходів має свої обмеження і ризики: живі методи чутливі до часу та стану системи, апаратні інтервенції можуть бути заблоковані механізмами Boot Guard або вимагати фізичного впливу на плату [2], а сайд-канальні техніки потребують спеціального обладнання і високої кваліфікації.

Порівняльний аналіз виявляє, що живе зняття пам'яті залишається найефективнішим і найменш ризикованим засобом роботи з FDE-системами, особливо коли дослідник має доступ до розблокованої системи. Апаратні методи займають проміжне місце, забезпечуючи можливість глибшого аналізу за відсутності доступу до працюючої ОС, проте вимагають значно більших ресурсів та суворого контролю процесу. Сайд-канальні підходи поки що слугують доповненням, яке дозволяє підтвердити або звузити простір пошуку криптографічних матеріалів, але не є основним засобом отримання доказів. Таким чином, ефективність конкретної методики визначається умовами розслідування, рівнем захисту системи та технічними можливостями лабораторії [1, 2].

У практичному вимірі ефективність вибору методу залежить від оцінки трьох груп факторів: технічних можливостей об'єкта (наявність TPM, налаштування Secure/Boot Guard, доступність DCI), часових і ресурсних обмежень експертної групи, а також правових умов, що визначають допустимість інвазивних методів. На підставі аналізу доцільно формулювати робочий підхід, який починається з консервації стану та фіксації всіх доступних метаданих і артефактів на рівні образу, продовжується

негайною спробою живої фіксації пам'яті за наявності працюючої системи, і завершується оцінкою можливості апаратного втручання або застосування сайд-каналів як крайньої опції. Такий послідовний підхід дозволяє знизити ризик безповоротної втрати доказів і одночасно зберегти можливості для подальших глибших інтервенцій.

На основі проведеного огляду можна сформулювати кілька узагальнених рекомендацій для підвищення результативності цифрових досліджень за умов повного шифрування даних. Перш за все, необхідно приділяти особливу увагу швидкому визначенню стану системи та, за можливості, проведенню живої фіксації пам'яті до вимкнення пристрою. Далі доцільно створювати повні сектор-в-сектор образи носіїв, зберігаючи всі метадані для подальшого аналізу. Під час відсутності живого доступу варто оцінювати можливість використання апаратних методів, проте лише в умовах суворого документування та наявності дозволів. Сайд-канальні дослідження слід розглядати як допоміжний засіб, що може бути корисним у складних кейсах або при необхідності підтвердження результатів іншими методами.

Таким чином, повне шифрування диска радикально змінило підходи до цифрової криміналістики, перетворивши її на багатокомпонентну дисципліну, де технічні, аналітичні та юридичні аспекти нерозривно пов'язані між собою. Відповіддю на цей виклик стало поєднання «живих», апаратних і аналітичних методів, розробка нових протоколів роботи з зашифрованими носіями та поступовий перехід до інтелектуальних систем аналізу пам'яті й структур даних. Подальші дослідження мають бути спрямовані на створення стандартизованих процедур та інструментів, які забезпечать збереження доказів і водночас дадуть можливість ефективно досліджувати системи з повним шифруванням інформації.

## *Л*ітература

1. Zunaidi M., Sayakkara A., Scanlon M. A Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices // International Journal of Digital Forensics and Incident Response. 2024.

2. Bichara de Assumpçao M., Reis M., Marcondes M. Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI // Digital Forensic Research Workshop (DFRWS). 2023.