УДК: 004.056

А. М. Міхеєв

Л. О. Майданевич

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ БЕЗПЕЧНОГО ВИВЕДЕННЯ З ЕКСПЛУАТАЦІЇ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ: ЧАСТИНА 2. ТЕХНІЧНІ ЗАСОБИ

Вінницький Національний Технічний Університет

Abstract

This paper examines the technical methods and tools for secure decommissioning of hardware and software systems. The study analyzes software overwriting (Clear), hardware sanitization via ATA Secure Erase and NVMe Sanitize commands (Purge), cryptographic erasure (Crypto Erase), and physical destruction (Destroy) in accordance with NIST SP 800-88r2 and IEEE 2883-2022. The applicability of each method is assessed depending on the storage medium type and data sensitivity level.

Анотація

У тезах розглянуто технічні методи та засоби безпечного виведення з експлуатації апаратно-програмних засобів (АПЗ). Проаналізовано методи програмного перезаписування (Clear), апаратного очищення за допомогою команд ATA Secure Erase та NVMe Sanitize (Purge), криптографічного стирання (Crypto Erase) і фізичного знищення носія (Destroy) відповідно до стандартів NIST SP 800-88r2 та IEEE 2883-2022. Оцінено застосовність кожного методу залежно від типу носія та рівня конфіденційності даних.

Ключові слова: *виведення з експлуатації, знищення даних, програмне перезаписування, ATA Secure Erase, NVMe Sanitize, криптографічне стирання, фізичне знищення, інформаційна безпека.*

Вступ

Виведення з експлуатації апаратно-програмних засобів потребує не лише організаційно-правового забезпечення, розглянутого в першій частині дослідження, а й застосування конкретних технічних методів знищення залишкових даних. Вибір методу санації носія безпосередньо визначає реальний рівень захисту інформації: застосування застарілих або невідповідних методів може залишити дані відновлюваними навіть після формального виведення АПЗ з обігу.

Метою цього дослідження є систематизація актуальних технічних методів безпечного виведення АПЗ з експлуатації відповідно до стандартів NIST SP 800-88r2 та IEEE 2883-2022 з урахуванням особливостей різних типів носіїв інформації.

Основна частина

Технічні методи знищення інформації поділяють на програмні, апаратні та комбіновані. Вибір методу обумовлюється типом носія, рівнем конфіденційності даних та вимогами застосовного стандарту [1, 2].

Програмний перезапис (рівень Clear). Метод полягає у заповненні всіх адресованих секторів носія псевдовипадковою послідовністю або нулями. NIST SP 800-88r2 відносить його до рівня Clear і вважає достатнім для носіїв із несекретними даними за умови подальшого використання в контрольованому середовищі [1]. Для HDD метод є практично ефективним, оскільки архітектура магнітного диска дозволяє адресувати всі сектори через стандартний інтерфейс ОС. Для SSD ситуація принципово інша: механізм

вирівнювання зносу (wear leveling) та резервування ємності (over-provisioning) унеможливлюють гарантований перезапис усіх фізичних комірок через стандартний інтерфейс, що робить метод Clear недостатнім для накопичувачів на основі флеш-пам'яті [3].

Апаратне очищення (рівень Purge). Для SSD та NVMe-накопичувачів рівень Purge досягається за допомогою команд ATA Secure Erase або NVMe Sanitize, які ініціюють вбудований алгоритм контролера накопичувача, що охоплює всі фізичні комірки, включно з ділянками over-provisioning [2]. Стандарт IEEE 2883-2022 класифікує команду NVMe Format NVM як більш надійну альтернативу для сучасних накопичувачів і уточнює умови її застосування [2]. Практична складність методу полягає у залежності від підтримки відповідних команд конкретним контролером та коректності їх реалізації виробником.

Криптографічне стирання (Crypto Erase). Застосовується для накопичувачів із повним апаратним шифруванням (Self-Encrypting Drive, SED) або томів із програмним шифруванням (BitLocker). Знищення ключа шифрування робить зашифровані дані математично невідновлюваними [1]. IEEE 2883-2022 визнає Crypto Erase методом санації категорії Purge за умови відповідності алгоритму шифрування (AES-128 або вище) та відсутності збережених резервних копій ключа [2]. Метод є особливо ефективним для хмарних середовищ, де фізичний доступ до носіїв обмежений, однак є непридатним, якщо накопичувач не підтримував шифрування до початку запису даних.

Фізичне знищення (рівень Destroy). Передбачає механічне подрібнення (шредування), демагнітизацію (дегаусінг) або плавлення носія і є єдиним методом з абсолютною гарантією невідновлюваності даних. NIST SP 800-88r2 рекомендує його для носіїв із матеріалами найвищого рівня конфіденційності або несправних накопичувачів, що не підтримують програмних методів санації [1]. Важливо враховувати, що дегаусінг є ефективним виключно для магнітних носіїв (HDD, стрічки) і не впливає на SSD та флеш-пам'ять. Фізичне знищення унеможливлює подальше використання носія та потребує документального підтвердження — складання акта або отримання сертифіката знищення від акредитованого підрядника.

Висновки

Технічні методи безпечного виведення АПЗ з експлуатації утворюють ієрархічну систему: від програмного перезаписування (Clear) для носіїв із загальнодоступними даними до фізичного знищення (Destroy) для носіїв із матеріалами найвищої конфіденційності. Ключовим принципом є відповідність методу типу носія: програмний перезапис є недостатнім для SSD, тоді як дегаусінг не діє на флеш-носії. Апаратні команди ATA Secure Erase та NVMe Sanitize є актуальними методами санації SSD відповідно до стандартів NIST SP 800-88r2 та IEEE 2883-2022. Криптографічне стирання є оптимальним методом для середовищ із попередньо зашифрованими носіями. Обов'язковим елементом усіх рівнів є документування виконаних процедур для забезпечення підзвітності та готовності до аудиту.

ЛІТЕРАТУРА

1. Kissel R., Regenscheid A., Scholl M., Stine K. Guidelines for Media Sanitization : NIST Special Publication 800-88 Rev. 2. Gaithersburg : NIST, 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf (дата звернення: 22.04.2025).
2. IEEE 2883-2022. IEEE Standard for Sanitizing Storage. New York : IEEE, 2022. URL: https://standards.ieee.org/ieee/2883/10600/ (дата звернення: 22.04.2025).
3. Wei M. et al. Reliably Erasing Data From Flash-Based Solid State Drives. FAST'11: Proceedings of the 9th USENIX Conference on File and Storage Technologies. San Jose : USENIX, 2011. P. 8.
4. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva : ISO, 2022. 27 p. URL: https://www.iso.org/standard/27001 (дата звернення: 22.04.2025).
5. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Київ : ДСТСЗІ СБ України, 2000. 21 с.

Міхеєв Артем Максимович – студент групи 1БС-22Б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: artikmih@gmail.com

Науковий керівник: Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Miheyev Artem Maksimovich – student of group 1BS-22b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: artikmih@gmail.com

Supervisor: Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com