УДК: 004.056

В. К. Маковейчук
Л. О. Майданевич

ВИВЕДЕННЯ З ЕКСПЛУАТАЦІЇ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Вінницький Національний Технічний Університет

Abstract
This paper examines the organizational and legal framework for the secure decommissioning of hardware and software systems. The study identifies key regulatory documents, institutional responsibilities, and internal policy requirements that form the foundation of a secure decommissioning process.
Keywords: *decommissioning, hardware, software, information security, data protection, organizational measures.*

Анотація
У тезах розглянуто організаційно-правову базу безпечного виведення з експлуатації апаратно-програмних засобів. Проаналізовано ключові нормативно-правові документи, розподіл відповідальності та вимоги до внутрішньої документації організації.
Ключові слова: *виведення з експлуатації, апаратно-програмні засоби, інформаційна безпека, захист даних, організаційні заходи.*

Вступ

Виведення з експлуатації апаратно-програмних засобів (АПЗ) є заключним, але критично важливим етапом їх життєвого циклу. Пристрої, що вибувають з обігу (жорсткі диски, твердотільні накопичувачі, флеш-носії тощо), можуть містити залишкові дані: конфіденційну інформацію, персональні дані або відомості з обмеженим доступом. Відтак, їх несанкціоноване розкриття через неналежне виведення АПЗ несе юридичні та репутаційні ризики для організації.

Формування чіткої організаційно-правової бази є першим і необхідним кроком у забезпеченні безпечного виведення АПЗ з експлуатації. Метою цього дослідження є аналіз нормативно-правових документів та організаційних вимог, що регулюють зазначений процес в Україні з урахуванням міжнародних стандартів.

Основна частина

Організаційно-правове регулювання виведення АПЗ з експлуатації в Україні спирається насамперед на Закон України «Про захист інформації в інформаційно-комунікаційних системах», який встановлює загальні вимоги до захисту інформації протягом усього її життєвого циклу, включаючи знищення [1]. Закон України «Про захист персональних даних» зобов'язує операторів персональних даних забезпечувати їх безпечне знищення після завершення строку обробки [2]. Вказані закони формують обов'язкову законодавчу базу для будь-якої організації, що здійснює обробку інформації з обмеженим доступом.

На рівні міжнародних стандартів ключовим документом є ISO/IEC 27001:2022 (Інформаційна безпека, кібербезпека та захист конфіденційності. Вимоги), який безпосередньо регламентує процедури виведення засобів зберігання даних з експлуатації [3]. Деталізовані рекомендації щодо методів очищення містяться у стандарті NIST SP 800-88 Rev. 1 [4]. Цей Стандарт визначає три рівні: Clear (програмне перезаписування), Purge (апаратне або криптографічне знищення) та Destroy (фізичне знищення носія). Вибір рівня залежить від категорії даних та ступеня їх конфіденційності.

Ефективне виведення АПЗ потребує чіткого розподілу відповідальності: керівництво затверджує рішення про виведення; служба інформаційної безпеки контролює знищення даних та визначає метод

очищення; ІТ-підрозділ виконує технічні процедури; юридична служба забезпечує відповідність правовим нормам; комісія зі списання оформлює відповідні акти.

Обов'язковою умовою є наявність внутрішньої нормативної документації: політики управління активами, регламентів роботи з носіями інформації та інструкцій щодо знищення даних. Класифікація АПЗ за ступенем конфіденційності оброблюваних даних визначає необхідний рівень заходів – від стандартного програмного очищення до фізичного знищення носія.

Важливим елементом є ведення реєстру АПЗ, що виводяться з експлуатації, із зазначенням інвентарного номера, типу пристрою, методу очищення даних, відповідального виконавця та дати процедури. Це забезпечує документальне підтвердження виконаних заходів і є необхідним під час аудиту інформаційної безпеки [5].

Висновки

Організаційно-правова база є фундаментом безпечного виведення АПЗ з експлуатації. Чинне законодавство України у поєднанні зі стандартами ISO/IEC 27001:2022 та NIST SP 800-88 формує достатню нормативну основу для побудови ефективного процесу. Відсутність чіткого розподілу відповідальності, внутрішньої документації та реєстру АПЗ суттєво підвищує ризики витоку конфіденційної інформації. Сформована організаційно-правова база є підґрунтям для впровадження технічних заходів захисту інформації.

ЛІТЕРАТУРА

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. *URL:* https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 22.04.2025).
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *URL:* https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 22.04.2025).
3. *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).
4. Kissel R., Regenscheid A., Scholl M., Stine K. *Guidelines for Media Sanitization* : NIST Special Publication 800-88 Rev. 1. Gaithersburg : NIST, 2014. 66 p. *URL:* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (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.

Маковейчук Владислав Костянтинович – студент групи 1БКС-22Б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: *vladuslavkonstantinovich@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

Makoveychuk Vladyslav – student of group 1BKS-22b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: *vladuslavkonstantinovich@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