Forensic Identification of Vehicles in Cases of VIN Manipulation: Modern Challenges and Approaches

Roman Pertsev
Ph. D. in Law, Head of the District Forensic Division of the Israel Police, Israel,
ORCID: https://orcid.org/0000-0001-9471-2962, e-mail: romanpertsev82@gmail.com

Vehicle identity falsification represents a key element of modern vehicle-related crime, particularly in cases involving organized and transnational theft. The increasing technological complexity of vehicles significantly affects forensic identification processes. This paper examines current challenges in the field of vehicle identification, with a focus on hybrid VIN forgery methods that combine physical alterations with the modification of digital data.
Keywords: *vehicle theft; VIN manipulation; forensic identification; digital forensics; automotive systems.*

Криміналістична ідентифікація транспортних засобів у випадках маніпуляцій з VIN-кодом: сучасні виклики та підходи

Роман Перцев

Фальсифікація ідентифікаційних даних транспортних засобів є невід'ємним елементом сучасної злочинності, пов'язаної з транспортними засобами, особливо у справах про організовані та транснаціональні крадіжки. Технологічна складність транспортних засобів, що зростає день у день, суттєво впливає на процеси криміналістичної ідентифікації. Розглянуто сучасні виклики у сфері ідентифікації транспортних засобів з особливим акцентом на гібридних методах підробки VIN-коду, що поєднують фізичні зміни з модифікацією цифрових даних.
Ключові слова: *крадіжка транспортного засобу; маніпуляція з VIN-кодом; криміналістична ідентифікація; цифрова криміналістика; автомобільні системи.*

Vehicle theft has evolved into a complex multi-stage criminal process in which concealment of vehicle identity plays a central role. The effectiveness of such criminal activity depends not only on the act of theft itself but on the ability to falsify identification data and reintroduce vehicles into legal circulation.

The Vehicle Identification Number (VIN) serves as the primary identifier linking a vehicle to registration systems, ownership records, and law enforcement databases [1]. Consequently, manipulation of VIN data remains one of the most effective methods used to conceal stolen vehicles.

Modern vehicles have transformed into complex cyber-physical systems integrating electronic control units (ECUs), telematics platforms, and cloud-based infrastructures. This transformation significantly alters the nature of forensic identification.

Traditional VIN manipulation techniques were based on direct physical alteration of identification markings, including re-stamping, grinding, and replacement of VIN plates.

Modern criminal practices demonstrate a transition toward more sophisticated approaches, including structural modification of vehicle components, use of donor vehicles, and integration of authentic VIN-bearing elements into altered vehicles.

A particularly complex situation arises when original VIN components from another vehicle are used. In such cases, the identification number may be genuine, while its association with the vehicle is falsified.

Modern vehicles store identification-related data across multiple digital systems, including ECUs, event data recorders, telematics modules, and cloud-based services.

These systems contain VIN-related identifiers and operational data. However, digitalization introduces new risks, including unauthorized access and manipulation of vehicle data [2; 3].

As a result, vehicle identity becomes distributed across physical and digital environments.

Thus, vehicle identification should be viewed as a multi-level process involving physical, structural, digital, and database elements.

Traditional forensic methods rely on microstructural deformations in metal; however, modern technologies, such as heat treatment or the replacement of structural components, can eliminate these traces [4].

Analysis of structural changes requires examination of welds, joints, and manufacturing characteristics.

Digital challenges include limited access, proprietary formats, and a lack of standardization.

From an evidentiary standpoint, inconsistencies between levels of identification are key indicators of tampering.

Thus, identifying a vehicle after a VIN has been forged presents a complex challenge for forensic analysis.

Modern forgery methods are multi-layered and require a comprehensive approach that combines:

- physical inspection,
- structural analysis,
- digital forensics,
- database checks.

There is a need to improve methodologies, expand access to vehicle data, and strengthen cooperation among forensic institutions.

References

1. NHTSA. Vehicle theft prevention standard (49 CFR Part 541). Washington, DC, 2023 [Electronic resource]. URL: https://www.regulations.gov/document/NHTSA-2023-0003-0001 (date accessed: 12.04.2026).
2. ENISA. Cybersecurity of connected and smart cars. 2024. DOI: 10.2824/0401593 (date accessed: 12.04.2026).
3. Checkoway S., et al. Comprehensive experimental analyses of automotive attack surfaces. *Proceedings of the USENIX Security Symposium*. 2011. Pp. 77–92.
4. Rak R., Kopencova D., Felcan M**.** Digital vehicle identity – digital VIN in forensic and technical practice. *Digital Investigation*. 2021. Vol. 39. Art. 301307. DOI: 10.1016/j.fsidi.2021.301307 (date accessed: 12.04.2026).