Comparative Analysis of Smart Lock Breaching Methods and Their Forensic Examination in Ukraine and the USA

Roman Pidnebennyi *

* LLC Undersky Locksmith, New York, USA, e-mail: underskylock@gmail.com

DOI: 10.32353/khrife.1.2025.12 UDC 343.98(477+73)
Received: 28.02.2025 / Reviewed: 05.03.2025 / Accepted for print: 26.03.2025 /
Available online: 31.03.2025

The development of technology has contributed to changes in methods of securing residential and commercial premises. Smart locks have become an integral part of the modern security market and have attracted the attention not only of property owners and security companies but also of criminals. The key methods of smart lock hacking used in Ukraine and the USA are examined, as well as the differences in forensic examination approaches to such crimes in these countries. A comparative analysis of physical, mechanical, and digital attacks has been conducted, outlining new challenges in the forensic examination of electronic locks and proposing recommendations for improving forensic research in this field. Modern security systems, including smart locks, combine mechanical and electronic technologies. At the same time, they are somewhat vulnerable, making them attractive to cybercriminals and traditional methods of physical hacking. The lack of a unified approach to forensic examination of such crimes in Ukraine and the USA creates difficulties in law enforcement activities. The purpose of this article is to explore the methods of smart lock hacking, compare the peculiarities of forensic examinations of such hacks in Ukraine and the USA, and propose measures to improve the investigation of such crimes. To achieve the stated goal, the method of comparative analysis, the traceological method of examining traces of hacking, the analysis of digital evidence, and vulnerability testing methods (fuzzing, reverse engineering of lock software) were applied.

Keywords: *smart locks; forensic examination; digital hacking; physical hacking; security; forensic analysis.*

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by *Roman Pidnebennyi*, proofreaded by *Daryna Dukhnenko*). The authors acknowledge translation as corresponding to the original.

Research Problem Formulation

Modern security systems, including smart locks, combine mechanical and electronic technologies. At the same time, they are somewhat vulnerable, making them attractive to cybercriminals and traditional methods of physical hacking[1]. The lack of a unified approach to the forensic examination of such crimes in Ukraine and the USA creates difficulties in law enforcement activities, making the resolution of this issue relevant in the modern innovative world.

Article Purpose

To study the methods of smart lock hacking, compare the specifics of forensic examinations of such hacks in Ukraine and the USA, and propose measures to improve the investigation of such crimes.

Research Methods

The method of comparative analysis, the traceological method of examining traces of hacking, the analysis of digital evidence, and vulnerability testing methods (fuzzing, reverse engineering of lock software) were applied.

Analysis of Essential Researches and Publications

The features of expert research on the hacking of mechanical and smart locks have been studied by scientists from Ukraine (B. Yakymenko [2], H. Hrabovskyi with co-authors [3], R. Kuznetsov and P. Yevseiev [4], V. Kopcha with co-authors [5]), as well as researchers from other countries (D. Ollam [6], S. Dashevskyi and F. La Spina [7],

1 Smith S. W., Oorschot P. C. van. The Internet of Things: Security Challenges. *IEEE Security and Privacy Magazine*. 2019. Art. 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918 (date accessed: 01.02.2025).

2 Якименко Р. В. Щодо важливості етапу порівняльного дослідження конформних слідів на деталях механічних сувальдних замків. *Криміналістика і судова експертиза.* 2018. Вип. 63. Ч. 1. С. 335—347. URL: https://digest.kndise.gov.ua/wp-content/uploads/2021/06/2018_1.pdf (date accessed: 01.02.2025).

3 Грабовський Г., Опарій А., Кузнєцов Р. Особливості експертного дослідження слідів знарядь злому. *Молодий вчений*. 2019. № 8 (72). С. 285—290. DOI: 10.32839/2304-5809/2019-8-72-61 (date accessed: 01.02.2025).

4 Кузнецов Р. В., Євсєєв П. О. Особливості трасологічного дослідження динамічних слідів знарядь зламу. *Аналітично-порівняльне правознавство*. 2022. № 4. С. 337—341. DOI: 10.24144/2788-6018.2022.04.61 (date accessed: 01.02.2025).

5 Копча В. В., Фрідманський Р. М., Копча Н. В. Правове дослідження слідів на місці злочину: які сприяють ефективному розкриттю і попередженню злочинів. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2022. Вип. 72. Ч. 2. С. 211—218. DOI: 10.24144/2307-3322.2022.72.67 (date accessed: 01.02.2025).

6 Ollam D. Practical Lock Picking: A Physical Penetration Tester's Training Guide. Syngress, 2010. 236 p.

7 Dashevskyi S., La Spina F. Old Code Dies Hard: Finding New Vulnerabilities in Old Third-Party Software Components and the Importance of Having SBoM for IoT / OT Devices / Black Hat Europe 2023. 48 p. URL: https://i.blackhat.com/EU-23/Presentations/EU-23-Dashevskyi-Old_code_dies_hard.pdf (date accessed: 01.02.2025).

D. dos Santos with co-authors [8], Y. Osawa and S. Higuchi [9]).

Main Content Presentation

With the advancement of technology, the number of threats related to lock hacking, both conventional and high-tech (including smart locks), is increasing and their quality is improving.

In the USA, significant attention is paid to the digital forensics of smart lock hacking (e. g., at the National Forensic Science Technology Center, hereinafter referred to as NIST [10]), whereas in Ukraine, forensic examinations are still predominantly focused on the physical analysis of mechanical lock breaches.

Popular smart lock brands in the USA: August, Yale, Schlage, Kwikset, Wyze. More common brands in Ukraine: Chinese models such as Xiaomi, Aqara, and low-cost OEM-solutions.

Authentication methods in the USA: Biometrics, PIN codes, NFC, Bluetooth, Wi-Fi [11], authentication methods in Ukraine: RFID-cards, PIN codes, mechanical keys.

Main vulnerabilities of smart locks in the USA: wireless signal interception, code guessing, attacks via mobile applications [12]. Main threats in Ukraine: mechanical breaches, power outages, outdated software.

Thus, since the methods of hacking mechanical and smart locks in the USA and Ukraine differ to some extent, the specifics of forensic examinations of such breaches will also vary, which we will examine in detail further.

Methods of Lock Hacking and Their Forensic Examination in the USA

It is worth noting that smart locks leave unique traces of unauthorized access — evidence such as:

- Access logs — saved records of locking (unlocking) events may contain

8 Santos D. dos, Guiot S., Dashevskyi S., Amri A., Kerro O. Route to Bugs: Analyzing the Security of BGP Message Parsing / Black Hat USA 2023. 33 p. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-dosSantos-Route-to-Bugs-Analyzing-the-Security-of-BGP.pdf (date accessed: 01.02.2025).

9 Osawa Y., Higuchi S. A Manufacturer's Post-Shipment Approach to Fend-Off IoT Malware in Home Appliances / Black Hat USA 2023. 37 p. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf (date accessed: 01.02.2025).

10 Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology. SP 800-86. U. S. Department of Commerce ; Technology Administration ; NIST, Aug 2006. 121 p. URL: https://surl.gd/bfuxct (date accessed: 01.02.2025) ; Ayers R., Brothers S., Jansen W. NIST Special Publication 800-101. Rev. 1. Guidelines on Mobile Device Forensics. U. S. Department of Commerce ; NIST, May 2014. 85 p. DOI: 10.6028/NIST.SP.800-101r1 (date accessed: 01.02.2025) ; Cybersecurity Subteam Recommendations / National Institute of Standards and Technology : website. 2023-08-18. 5 p. URL: https://surl.li/fkkmcm (date accessed: 01.02.2025).

11 Berrios J., Mosher E., Benzo S., Grajeda C., Baggili I. Factorizing 2FA: Forensic analysis of two-factor authentication applications. *Forensic Science International: Digital Investigation*. 2023. Vol. 45. Suppl. Art. 301569. DOI: 10.1016/j.fsidi.2023.301569 (date accessed: 01.02.2025).

12 Caballero-Gil C., Álvarez R., Hernández-Goya C., Molina-Gil J. Research on smart-locks cybersecurity and vulnerabilities. *Wireless Networks*. 2024. Vol. 30. Pp. 5905—5917. DOI: 10.1007/s11276-023-03376-8 (date accessed: 01.02.2025).

information about the time of the breach or attempts to enter an incorrect code.
- Bluetooth or Wi-Fi connection data — can provide insights into hacking tools used for signal interception or code guessing.
- Forensic analysis of mobile applications — if the lock is controlled via a smartphone, it is possible to trace interactions with the app, even if the attacker attempted to delete it.

Smart locks have gained widespread popularity due to their convenience and integration with smart home systems [13].

According to a 2023 study, 12 % of smart lock owners in the USA experienced attempted breaches of their devices. Main threats:
- physical hacking (43%) — 3D-printed lock picks, bumping, magnetic manipulation;
- cyberattacks (37%) — hacking mobile applications, intercepting wireless signals via Bluetooth or Wi-Fi;
- attacks on the authentication system (20%) – password hacking or manipulation of NFC-cards [14].

In 2023, the FBI IC3 received 2,825 complaints about ransomware attacks, causing losses exceeding $59.6 million [15]. Such programs encrypt data on a device, making it inaccessible to users, while cybercriminals demand a ransom for the return of the stolen information. There have been recorded cases where attackers targeted smart locks, blocking access to premises and using this as a tool for extortion. For example, in the Austrian *Romantik Seehotel Jäegerwirt,* hackers compromised the electronic key system, locked guests in their rooms, and demanded a ransom to restore access. This demonstrates the vulnerability of IoT devices (*Internet of Things*), particularly electronic lock systems, which can become targets for attacks, compromising user security and causing financial losses. According to the *2024 Consumer Cyber Readiness Report,* 7 % of registered cyberattacks in 2024 were related to ransomware attacks on smart home devices, including smart locks [16]. Participants of the *Black Hat USA 2023* and *DEF CON* conferences have once again [17] explored new attack methods on smart locks (including the use of 3D-printed lock picks and magnetic manipulation), as well as detection, prevention, and forensic investigation techniques for such attacks.

With the advancement of technology, both hacking methods and forensic investigation techniques are evolving. Tra-

13 Adaramola O. O., Odigbo Ch. S., Elelegwu D., Chen L. Safeguarding Smart Homes: A Digital Security and Digital Forensics Approach / ResearchGate : website. Feb 2025. 14 p. DOI: 10.13140/RG.2.2.19403.30240 (date accessed: 01.02.2025) ; Hutchinson Sh., Yoon Y. H., Shantaram N., & Karabiyik U. Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory. *2020 ASEE Virtual Annual Conference Content Access*. June 22—26. 2020. P. ID #29634. DOI: 10.18260/1-2--34868 (date accessed: 01.02.2025).

14 Federal Bureau of Investigation. Internet Crime Report 2023 / Internet Crime Complaint Center. Dec 12. 2023. Pp. 13—14. URL: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf (date accessed: 01.02.2025).

15 Ibid.

16 2024 Consumer Cyber Readiness Report / Aspen Digital : website. Oct 1. 2024. URL: https://www.aspendigital.org/report/2024-consumer-cyber-readiness-report/ (date accessed: 01.02.2025).

17 Black Hat USA 2023 (Aug 5—10, 2023; Mandalay Bay / Las Vegas + Virtual) / Black Hat : website. 2023. URL: https://www.blackhat.com/us-23/ (date accessed: 01.02.2025).

ditional mechanical locks leave physical traces of tampering, whereas smart locks may contain digital traces, the analysis of which requires specialized forensic examination.

Among the methods of smart lock hacking in the USA, digital attacks stand out the most, as they exploit vulnerabilities in software and network protocols [18]. The analysis of smart lock hacking in the USA is based on standardized digital forensics methodologies, which allow law enforcement agencies to accurately determine the circumstances of the breach, identify the method of unauthorized access, and trace the perpetrator.

For example, Bluetooth and Wi-Fi interception is used to decrypt transmitted data or clone authentication keys [19]. It has also been found that Bluetooth commands can be intercepted and replayed, granting unauthorized access to a lock without the need for a physical key. Most smart locks use *Bluetooth Low Energy (BLE)* or Wi-Fi to connect with the owner's smartphone. Attackers can exploit the following hacking methods:

- Bluetooth *connection interception* – hackers can record a communication session and attempt to replay it to gain access.
- Wi-Fi connection attacks – if the lock is connected to the internet, attackers can manipulate commands using Man-in-the-Middle (MITM) attacks.
- Brute-force attacks – cracking passwords or digital codes using automated scripts.

There are also other threats, such as:

- Software attacks (*API* vulnerabilities) – exploiting flaws in mobile applications that control smart locks [20]. Due to weak user authentication or with the use of specialized equipment, attackers can remotely intercept control signals between the mobile device and the lock.
- Unauthorized biometric data collection – a compromised smart lock modified by attackers can capture a user's fingerprints and transmit them via encrypted channels to a remote, controlled server without the owner's knowledge.
- Bypassing recognition algorithms – through "fingerprint replay" attacks, intercepted biometric data can be used to gain access to other devices owned by the victim.

This is why biometric data should be stored locally and protected using strong security mechanisms, such as *FIDO2* encryption (*Fast IDentity Online 2* – an open authentication standard designed to enhance user login procedures for improved security and trust in online services) [21].

18 Black Hat / DEF CON 2024: Latest Insights on Security and AI. ISMG Compendium Showcases More Than 50 Interviews on Threats, Emerging Solutions / Bank Info Security : website. Sept 13, 2024. URL: https://www.bankinfosecurity.com/black-hatdef-con-2024-latest-insights-on-security-ai-a-26283 (date accessed: 01.02.2025).

19 Winkelmann A. Unauthorized Smart Lock Access. Ethical Hacking of Smart Lock Systems. Stockholm, Sweden, 2022. 99 p. URL: https://kth.diva-portal.org/smash/get/diva2%3A1749555/FULLTEXT01.pdf (date accessed: 01.02.2025).

20 Ayers R., Brothers S., Jansen W. *Op. cit.* DOI: 10.6028/NIST.SP.800-101r1 (date accessed: 01.02.2025) ; Kent K., Chevalier S., Grance T., Dang H. *Op. cit.* URL: https://surl.gd/bfuxct (date accessed: 01.02.2025).

21 Kerrison S. IoT Droplocks: Wireless Fingerprint Theft Using Hacked Smart Locks. *ArXiv*. 2022. arXiv:2208.13343. DOI: 10.48550/arXiv.2208.13343 (date accessed: 01.02.2025).

Cases of physical tampering with the hybrid mechanisms of smart locks (such as 3D-printed lock picks and magnetic manipulation) are also common. In the USA, 3D-printed lock picks are widely used by physical security researchers and, unfortunately, also by malicious actors attempting to bypass traditional mechanical defenses [22]. Main methods of application:

- Key duplication – 3D-printing can create precise copies of keys based solely on their photographs or measurements.
- Lock core manipulation – printed lock picks can easily open cylinder mechanisms, which are widely used.
- Replacement of traditional lock picks – modern 3D-printing materials are strong enough to manipulate lock mechanisms.

At *the Black Hat USA 2019* conference, researchers demonstrated how 3D-printing can be used to create advanced lock-picking tools [23]. In particular, *L. Garland* and co-authors found that an analysis of artifacts generated during the 3D-printing process revealed digital traces at all studied stages [24]. These artifacts can be crucial for digital forensics, as they contain data related to the 3D-printer, slicing software, and G-code files. The study of digital traces in 3D-printing is particularly relevant in the context of security, especially when it comes to the illegal manufacturing of lock picking tools. As noted by *G. Hill* (2014), 3D-printed keys can be used to unlock complex locks within seconds, posing a serious security challenge [25].

Protection against 3D-printed lock picks is possible by using patented key profiles, which are harder to duplicate, and implementing multi-level pin systems, making unlocking with printed tools more difficult.

Security specialists have also observed magnetic interference with electromechanical locks and traditional models using magnetic keys. Attackers exploit powerful neodymium magnets to manipulate mechanical lock parts, bypass electronic lock components, and conduct reverse engineering of magnetic keys to create a functional duplicate without physical access to the original.

Strong magnets can bypass both electronic and mechanical locking mechanisms. At the Black Hat USA 2021, researchers confirmed that 54% of tested electronic locks were vulnerable to magnetic attacks, as they lacked proper shielding [26]. Protection methods: using non-magnetic alloys

22 Hill G. 3-D Printed Skeleton Key Can Open Almost Any Lock in Seconds / Security Today : website. Sep 03. 2014. URL: https://securitytoday.com/articles/2014/09/03/3d-printed-skeleton-key-can-open-almost-any-lock-in-seconds.aspx (date accessed: 01.02.2025) ; Four Ways 3D Printing May Threaten Security / RAND Corporation : website. May 8 2018. URL: https://www.rand.org/pubs/articles/2018/four-ways-3d-printing-may-threaten-security.html (date accessed: 01.02.2025).

23 Black Hat USA 2019 (Aug 3—8, 2019; Mandalay Bay / Las Vegas) / Black Hat : website. 2019. URL: https://www.blackhat.com/us-19/ (date accessed: 01.02.2025).

24 Garland L., Neyaz A., Varol C., & Shashidhar N. K. Investigating Digital Forensic Artifacts Generated from 3D Printing Slicing Software: Windows and Linux Analysis. *Electronics.* 2024. Vol. 13 (14). P. 2864. DOI: 10.3390/electronics13142864 (date accessed: 01.02.2025).

25 Hill G. Op. cit. URL: https://securitytoday.com/articles/2014/09/03/3d-printed-skeleton-key-can-open-almost-any-lock-in-seconds.aspx (date accessed: 01.02.2025).

26 Black Hat USA 2021 (Juli 31 — Aug 5, 2021; Mandalay Bay / Las Vegas + Virtual) / Black Hat : website. 2021. URL: https://www.blackhat.com/us-21/ (date accessed: 01.02.2025).

in critical lock components; implementing protective housings to shield against external magnetic influences; developing algorithms to detect unauthorized manipulations of electronic locks.

Thus, 3D-printed lock picks and magnetic manipulation are real threats to physical lock security in the USA. Forensic analysis of such crimes focuses on detecting residual traces of 3D-printed picks within lock mechanisms and analyzing the effects of magnetic interference.

Protection against lock hacking: combining electronic and mechanical security methods, using more complex key profiles, and employing magnet-resistant materials.

Methods of Lock Hacking and Their Forensic Analysis in Ukraine

In Ukraine, mechanical lock hacking remains the most common type of unauthorized access-related crime compared to digital breaches. The most widespread methods for mechanical locks include bumping, lock pick manipulation, drilling, and forced entry, all of which leave distinctive traces on lock components. As smart locks become increasingly popular, they are targeted by both physical and digital attacks, including wireless signal interception, exploitation of software vulnerabilities, and hacking of mobile applications.

R. Yakymenko provided a detailed analysis of mechanical lock hacking through conformal traces on lock components [27]. Bumping is a method of opening pin-cylinder locks without the original key by using a special bump key, which is inserted into the keyway and subjected to slight impacts, causing the lock's pins to jump, allowing the cylinder to rotate and unlock the mechanism. The analysis of bumping focuses on identifying conformal traces – distinctive microscopic damage on internal lock components caused by bump key impacts. Key forensic indicators include microscopic dents or scratches on pins and spool pins, uneven wear, or deformations on the contact surfaces.

High-precision microscopes and other forensic tools are used to detect such traces, allowing for a thorough examination of the internal components of the lock. Identifying these indicators is critically important for confirming unauthorized access through bumping, as external damage is usually absent. Including this analysis in forensic investigations helps law enforcement agencies more effectively investigate cases of illegal entry and hold offenders accountable.

The use of lock picks and drilling for lock manipulation is discussed in the textbook *Forensics* edited by V. Shepitko [28]. Lock picks are a set of specialized tools used to manipulate the internal mechanisms of a lock without using the original key.

Based on their function, lock picks can be classified as follows:

- Manual picks (special hooks, rakes, tension tools) allow the operator to individually adjust the position of pins in a pin tumbler lock.
- Automated picks (electronic or impact tools) operate by quickly determining the correct combination without requiring precise manual manipulation.

27 Якименко Р. В. Зазнач. твір. URL: https://digest.kndise.gov.ua/wp-content/uploads/2021/06/2018_1.pdf (date accessed: 01.02.2025).

28 Шепітько В. Ю., Коновалова В. О., Журавель В. А. та ін. Криміналістика : підручник / за ред. В. Ю. Шепітька. 4-те вид., перероб. і допов. Харків, 2008. С. 60—62, 71—72. URL: https://law.sspu.edu.ua/files/documents/books/library/17/shepitko.pdf (date accessed: 01.02.2025).

Lock picks leave characteristic conformal traces on the internal components of a lock, including:

- scratches and wear marks on pins and levers caused by repeated manipulation;
- uneven wear of the mechanism, indicating unusual damage or displacement of the pins;
- changes in spring tension due to forceful manipulation techniques.

The aforementioned damage serves as evidence in criminal investigations, as it helps determine the method and tools used for the breach, as well as distinguish specialized burglary tools from standard lock wear and tear.

Drilling is one of the most destructive lock-breaking methods, involving the physical destruction of the lock's mechanism, allowing it to be opened without the original key.

The typical drilling points depend on the lock's design:

- drilling the cylinder – destroys the pin mechanism in pin tumbler locks;
- drilling near the bolt – used on lever locks and electromechanical locks to forcefully unlock the mechanism.

Forensic analysis of drilling:

- drill holes – their diameter, shape, and positioning can provide information about the tool used for the breach;
- metal shavings – indicate drilling patterns and direction, helping reconstruct the perpetrator's actions;
- thermal damage – caused by high-speed drills or tools with increased friction.

Criminals frequently use drilling to break into safes, electromechanical systems, and high-security locks, as it allows them to quickly bypass complex mechanisms without requiring advanced skills like lock picking.

Thus, mechanical lock breaches remain more relevant in Ukraine.

Analysis of Mechanical Break-In Traces

Mechanical break-in analysis is a key aspect of forensic criminology, as it allows experts to:

- determine the break-in method – whether lock picks or forceful methods like drilling were used;
- identify the criminal's tools – the type of damage can indicate a specific type of lock pick or drill, helping link it to suspects;
- assess the skill level of the perpetrators – professional burglaries often leave minimal damage, whereas amateur attempts cause more visible traces;
- confirm or refute unauthorized entry – a lack of break-in traces may indicate staged tampering.

The use of modern technologies, such as 3D-scanning of microscopic damage and spectral analysis of metal particles, allows for more precise forensic examinations. Experts consider the development of 3D-forensics essential for advancing crime investigation practices [29].

Thus, traceological analysis of break-in marks left by burglary tools remains a key stage in forensic investigations of lock-related crimes in Ukraine. Main types of traces that can be detected on a lock's body or internal mechanism:

29 Дуфенюк О. М. Майбутнє 3D криміналістики: інновації, які змінюють практику досудового розслідування. *Юридичний науковий електронний журнал*. 2024. № 3. С. 457—460. DOI: 10.32782/2524-0374/2024-3/110 (date accessed: 01.02.2025).

- deformation marks – dents, scratches, bends on the metal casing or cylinder;
- dynamic impact traces – friction or displacement caused by levers, screwdrivers, crowbars, or specialized lock-picking tools;
- micro-damage to the internal mechanism – possible evidence of manipulative break-in techniques, such as bumping or electronic attacks.

According to the study by H. Hrabovskyi and co-authors [30], traceological analysis of break-in marks is conducted using optical microscopes and digital tools to determine the mechanism of damage formation and the type of tool used for the break-in.

Regarding dynamic break-in traces, they contain crucial information for reconstructing the lock-breaking mechanism and identifying the type of tool applied. R. Kuznetsov and P. Yevseiev highlight the following key parameters for analysis:

- depth and shape of scratches – indicate the type of tool used (e.g., crowbar, screwdriver, hammer);
- angle and direction of movement – help determine how force was applied during the break-in;
- presence of metal residues – may indicate contact with specialized break-in tools [31].

Computer-based traceological modeling enables precise reconstruction of break-ins, allowing forensic experts to compare identified marks with known burglary tools commonly used in criminal activities.

Thus, the study of mechanical break-in traces on smart locks is crucial for identifying penetration methods and the tools involved. Combining traceological analysis, computer modeling, and legal support enhances forensic accuracy and improves investigation efficiency. However, unlike the USA, where demand for smart locks is rapidly growing, their adoption in Ukraine remains relatively low, and digital attacks on locks are still rarely recorded. Meanwhile, a lack of software updates and weak encryption standards in widely used Chinese smart lock models poses serious security risks.

Analysis of Digital Break-in Traces

The analysis of smart lock breaches in the USA is based on standardized digital forensic methodologies, allowing law enforcement to accurately determine the circumstances of the breach, identify unauthorized access methods, and trace the perpetrator.

Modern forensics in the USA treats digital traces as full-fledged evidence, equivalent to traditional physical traces such as fingerprints or tool marks.

Key principles of collecting and analyzing digital evidence:

- *integrity* – evidence must not be altered or damaged during collection;
- *authenticity* – it must be proven that the collected digital traces are directly related to the specific criminal incident;
- *reproducibility* – independent experts should be able to repeat the analysis and obtain the same results;

30 Грабовський Г., Опарій А., Кузнєцов Р. Зазнач. твір. DOI: 10.32839/2304-5809/2019-8-72-61 (date accessed: 01.02.2025).

31 Кузнєцов Р. В., Євсєєв П. О. Зазнач. твір. DOI: 10.24144/2788-6018.2022.04.61 (date accessed: 01.02.2025).

- *chain of custody* – a documented record must be kept of who accessed the digital evidence, when, and how.

During smart lock breach investigations in the USA, traditional forensic methods are combined with digital forensics techniques.

Modern smart lock event logs store information about:

- the date and time of each unlocking/locking event;
- attempts to enter an incorrect code or connect an unauthorized device;
- system reboots or password changes.

Law enforcement can retrieve this information directly from the lock or from the manufacturer's servers. In the USA, legal precedents allow authorities to access these records through court orders under the *Stored Communications Act (SCA, 1986)*, which governs access to electronic communications.

Methods of log analysis:

- *Forensic Imaging* – creating an exact copy of the event log for further analysis without modifying the original data;
- *Timeline Analysis* – examining the sequence of events to detect suspicious activity (e.g., login attempts at unusual times or from unknown devices);
- *Correlation with Other Sources* – comparing lock data with Wi-Fi router logs, surveillance footage, and mobile network records.

Most smart locks connect to the owner's smartphone via BLE (Bluetooth Low Energy) or Wi-Fi. In the event of a breach, the following forensic analysis methods are used:

- *Radio Frequency (RF) Traffic Analysis* – using specialized tools such as Wireshark or HackRF to intercept communication signals;
- *Router Forensics* – examining Wi-Fi connection logs to determine if an unauthorized device was used for the break-in;
- *Bluetooth Log Recovery* – using software such as BLE Sniffer to analyze past connections.

Smart locks are controlled via a mobile application, which may contain valuable information about device usage and potential breaches. In the USA, digital forensics tools are used to extract and analyze mobile device data, including: *Cellebrite UFED* – professional software for extracting data from smartphones. *Magnet AXIOM* – enables analysis of activity logs within the smart lock's mobile application.

Autopsy (The Sleuth Kit) is an open-source tool used for analyzing smartphone data in forensic investigations. Analysis methods:

- decoding mobile app log files – extracts information on login attempts, connection errors, password resets, etc.;
- checking cached data – even after the app is deleted, some data may remain in device memory;
- correlation with GPS data – helps determine whether the lock owner was physically near the location at the time of the breach or if the lock was hacked remotely.

Many smart locks synchronize their data with the manufacturer's server, allowing forensic investigators to retrieve additional digital evidence. User activity logs record all changes in the security system, while the firmware update history can reveal whether a known exploit was used in the breach. If the lock was hacked remotely, traces of the attack, such as the hacker's IP addresses, may remain on the server. Law enforcement agencies in the U.S. can request access to this data under the *Stored*

Communications Act by submitting an official request to the manufacturer. Methods for analyzing server data:

- access logs – reviewing login records and attempts to change settings;
- network request analysis – identifying unknown IP addresses or suspicious API requests to the lock;
- forensic analysis of SQL databases – recovering the lock's usage history.

Let's summarize the key points. In the United States, a comprehensive approach is used to analyze smart lock breaches, incorporating various digital forensic methods such as log analysis, connection tracking, mobile app forensics, and server data investigation. A well-established legal framework regulates the collection and use of digital evidence in criminal cases. Additionally, law enforcement agencies have access to advanced forensic tools, professional equipment, and specialized software for breach analysis. In contrast, Ukraine currently lacks a structured methodology, making it significantly more challenging to effectively investigate digital breaches. To combat digital lock hacking more effectively, Ukraine should adopt best practices from U.S. digital forensics and implement appropriate legal mechanisms at the legislative level.

Challenges in Analyzing Smart Lock Breaches in Ukraine Compared to the U.S.

Based on the aforementioned points, the key challenges in analyzing smart lock breaches in Ukraine compared to the U.S. include:

- *Limited specialization of experts.* In the U.S., smart lock breaches are analyzed not only by traditional forensic experts but also by cybersecurity specialists, ethical hackers, and IoT experts. In Ukraine, this field is still developing, and the number of experts capable of conducting a comprehensive analysis of digital traces remains limited.
- *Lack of standardized digital forensics methodologies.* The U.S. has standardized methodologies for analyzing digital evidence, such as NIST recommendations. While Ukraine adopts some international best practices, it still lacks a unified approach to cybercrime analysis, particularly regarding smart lock breach investigations.
- *Limited access to specialized equipment.* U.S. investigators have access to advanced digital forensic tools (logic analyzers, data extraction software, etc.) and specialized forensic laboratories. In Ukraine, such resources are significantly more limited, complicating the analysis of modern electronic lock breaches.
- *Insufficient legal framework for digital forensics.* In the U.S., digital forensic analysis is governed by established laws, allowing digital evidence to be used in court. Key regulations cover both hacking methods and legal liability for unauthorized access to IoT devices, including electronic locks.

Key U.S. regulations related to smart lock breach investigations:

- *Federal Rules of Evidence (1975)* establish that digital data, including smart lock access logs, network logs, and breach traces, are admissible as evidence in court proceedings.
- *Computer Fraud and Abuse Act (CFAA, 1986, updated 2023)* criminalizes unauthorized access to computer systems, including hacking attempts on IoT devices.

- *Electronic Communications Privacy Act (ECPA, 1986, updated 2018)* regulates law enforcement access to electronic communications and cloud storage where smart lock data may be stored.
- *Cybersecurity Information Sharing Act (CISA, 2015)* facilitates the exchange of cybersecurity threat information between government agencies and private companies, which can be applied to analyzing smart lock attacks.
- *Federal Trade Commission Act (FTC Act, 1914, updated 2021)* allows investigations into cases where smart lock manufacturers fail to provide adequate security, leading to breaches or data leaks.
- *California Consumer Privacy Act (CCPA, 2018)* governs the use and storage of personal data, including information collected by smart locks (biometric data, access logs, etc.).

The combination of these regulations forms a legal foundation for investigating smart lock breaches in the U.S.

In Ukraine, the legal aspects of using electronic evidence in criminal cases are still in their infancy, which often results in courts rejecting such evidence due to the lack of a clear procedure for its documentation and preservation. This makes the analysis of digital traces problematic due to several factors [32], including:

- The *Criminal Procedure Code of Ukraine* [33] does not provide a clear definition of electronic evidence in criminal proceedings. This creates legal uncertainty regarding the proper collection and use of digital evidence obtained from smart locks.
- Lack of standardized procedures for digital trace analysis. While the U.S. follows established NIST methodologies, Ukraine is still in the process of developing similar standards.
- Limited access to smart lock logs and data. If the smart lock manufacturer is based abroad (which is often the case), Ukrainian investigators face difficulties obtaining user access logs.
- Insufficient technical infrastructure. Only a few forensic laboratories in Ukraine have access to modern software for analyzing digital devices.
- Courts often reject digital evidence due to improper documentation or the lack of expert verification.

In our opinion, the implementation of the principles of the *Berkeley Protocol* [34] in Ukrainian practice could contribute to the standardization of processes for handling electronic evidence. This involves ensuring the authenticity and integrity of digital data, which is critically important in investigating cybercrimes, particularly smart lock breaches. However, for

32 Черемнова А. І., Белік Л. С. Цифрова інформація як об'єкт експертного дослідження в умовах діджиталізації: проблеми та перспективи розвитку. *Криміналістика і судова експертиза*. 2023. Вип. 68. С. 57—65. DOI: 10.33994/kndise.2023.68.06 (date accessed: 01.02.2025).

33 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 06.01.2025).

34 Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (date accessed: 01.02.2025).

the effective implementation of these principles, it is necessary to introduce appropriate amendments to the Criminal Procedure Code of Ukraine, clearly defining the concept of "electronic evidence" and the procedures for its processing [35].

Unlike the United States, Ukraine has a significantly higher number of cases involving the use of cheap or illegally imported smart locks that lack necessary security protocols. This makes them more vulnerable to hacking while also complicating forensic examinations, as official documentation is unavailable and manufacturers do not cooperate with law enforcement agencies.

One of the key security risks for smart locks is the use of outdated third-party software components that may contain undiscovered vulnerabilities. According to research by S. Dashevskyi and F. La Spina, many IoT devices incorporate components that have not been updated for years, creating far greater opportunities for cybercriminal attacks [36].

A study of Sierra Wireless AirLink devices identified 21 new vulnerabilities, 15 of which were related to third-party software libraries. This underscores the necessity of regular software audits and maintaining an up-to-date Software Bill of Materials (SBoM) [37].

The analysis of smart lock hacking methods requires a comprehensive approach that considers forensic, cybersecurity, and legal aspects. In the United States, this process is well-established due to collaboration between law enforcement agencies, cybersecurity experts, and the security industry. In Ukraine, however, forensic examination of smart locks faces several challenges, including a lack of personnel, methodological standards, technical capabilities, and legal mechanisms. To improve the situation, it is necessary to enhance expert training, adapt international methodologies, and refine the regulatory framework for digital forensics.

For effective identification of vulnerabilities in *IoT* device software, including smart locks, researchers utilize fuzz testing. As noted by *D. dos Santos* and colleagues, this method allows for the detection of weaknesses in the implementation of hardware and network protocols, which can also be applied to smart lock security analysis [38].

Fuzz testing enables the automatic generation of thousands of incorrect requests, helping to identify critical vulnerabilities in smart lock software during the development stage.

Another approach to improving IoT device security is presented in the research by Y. Osawa and S. Higuchi, which describes the *ASTIRA* system (an intelligent platform) used for collecting and analyzing attacks on IoT devices, including smart locks [39].

Key measures to enhance smart lock security include:

- deploying honeypots – specially configured devices with vulnerabilities

35 Черемнова А. І., Бєлік Л. С. Зазнач. твір. С. 57, 59—60. DOI: 10.33994/kndise.2023.68.06 (date accessed: 01.02.2025).

36 Dashevskyi S., La Spina F. Op. cit. URL: https://i.blackhat.com/EU-23/Presentations/EU-23-Dashevskyi-Old_code_dies_hard.pdf (date accessed: 01.02.2025).

37 Ibid.

38 Santos D. dos, Guiot S., Dashevskyi S., Amri A., Kerro O. Op. cit. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-dosSantos-Route-to-Bugs-Analyzing-the-Security-of-BGP.pdf (date accessed: 01.02.2025).

39 Osawa Y., Higuchi S. Op. cit. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf (date accessed: 01.02.2025).

that serve as decoys to collect information about attacks;
- automating malware analysis to detect new threats at early stages;
- establishing a centralized database of IoT device attacks, enabling manufacturers to respond more quickly to emerging threats.

According to researchers, over the past five years, more than 2.2 billion attacks on IoT devices have been recorded, highlighting the need for continuous smart lock security monitoring [40].

Based on the information provided above, several key recommendations can be highlighted to enhance smart lock security:
- conducting regular software audits to check all third-party components for vulnerabilities [41];
- implementing fuzz testing during smart lock development to identify potential weaknesses [42];
- utilizing IoT attack monitoring systems (such as ASTIRA) to detect and analyze emerging threats [43];
- ensuring SBoM (Software Bill of Materials) support by documenting all software components to enable quick updates of vulnerable libraries [44].

The analysis of software vulnerabilities in smart locks plays a crucial role in forensic investigations of crimes related to electronic access system breaches. Fuzz testing not only enables manufacturers to enhance device security but also allows forensic experts to reconstruct potential hacking scenarios and identify exploits used by criminals. Attack monitoring systems, such as *ASTIRA*, can detect intrusion attempts in real time, providing valuable evidence in criminal cases. Creating a centralized database of attacks on IoT devices helps experts recognize common hacking methods and connect separate crimes. Additionally, analyzing access logs and digital traces left by vulnerable smart locks serves as key evidence in court proceedings. Thus, implementing methods for detecting and mitigating vulnerabilities improves forensic examination efficiency and aids law enforcement in investigating digital security breaches.

In modern forensic science, technical prevention measures play a significant role in crime prevention and evidence collection. These measures include security surveillance systems, electronic access controllers, and chemical markers. Their implementation not only complicates criminal activities but also contributes to the creation of additional traces when criminals attempt to bypass these measures. This increases the amount of forensic evidence available for investigation. For example, when interacting with complex security systems, a perpetrator may leave traces at the crime scene that can help identify their identity or the tools

40 Osawa Y., Higuchi S. Op. cit. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf (date accessed: 01.02.2025).

41 Dashevskyi S., La Spina F. Op. cit. URL: https://i.blackhat.com/EU-23/Presentations/EU-23-Dashevskyi-Old_code_dies_hard.pdf (date accessed: 01.02.2025).

42 Santos D. dos, Guiot S., Dashevskyi S., Amri A., Kerro O. Op. cit. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-dosSantos-Route-to-Bugs-Analyzing-the-Security-of-BGP.pdf (date accessed: 01.02.2025).

43 Osawa Y., Higuchi S. Op. cit. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf (date accessed: 01.02.2025).

44 Dashevskyi S., La Spina F. Op. cit. URL: https://i.blackhat.com/EU-23/Presentations/EU-23-Dashevskyi-Old_code_dies_hard.pdf (date accessed: 01.02.2025).

used in the breach. Therefore, integrating modern technical prevention measures not only enhances security levels but also improves the effectiveness of forensic investigations [45].

Conclusions

The demand for smart locks in both the U.S. and Ukraine has been growing annually, along with the number of attempts to compromise them. Analysis of attack methods indicates that digital attacks are more common in the U.S., while physical manipulations dominate in Ukraine. Smart locks are vulnerable to both mechanical and digital breaches. Implementing fuzz testing and utilizing honeypots can enhance the security of smart locks. Their protection should combine both physical and digital security measures to minimize hacking risks and improve the effectiveness of criminal investigations. The analysis of smart lock attacks can also benefit from artificial intelligence, the creation of a unified database of smart lock connection logs, advancements in digital forensics, specialized training for experts, and the integration of U.S. forensic standards into national legislation.

Порівняльний аналіз методів зламу смартзамків і їхньої криміналістичної експертизи в Україні та США

Роман Піднебенний

Розвиток технологій сприяв зміні методів убезпечення житлових і комерційних приміщень. Смартзамки стали невід'ємною складовою сучасного ринку безпеки і привернули увагу не лише власників нерухомості та охоронних фірм, а й злочинців. Розглянуто ключові методи зламу смартзамків, застосовуваних в Україні та США, відмінності в підходах до криміналістичної експертизи таких злочинів у цих країнах. Проведено порівняльний аналіз фізичних, механічних і цифрових атак, окреслено нові виклики у сфері судової експертизи електронних замків та запропоновано рекомендації щодо вдосконалення криміналістичних досліджень у цій галузі. Сучасні системи безпеки, зокрема смартзамки, поєднують механічні й електронні технології. Водночас вони певною мірою вразливі, що робить їх привабливими для кіберзлочинців і традиційних методів фізичного зламу. Відсутність єдиного підходу до криміналістичної експертизи цих злочинів в Україні та США створює труднощі у правоохоронній діяльності. Мета статті — дослідити методи зламу смартзамків, порівняти особливості криміналістичних експертиз подібних зламів в Україні та США й запропонувати заходи для вдосконалення розслідування таких злочинів. Для досягнення поставленої мети застосовано метод порівняльного аналізу, трасологічний метод експертизи слідів зламу, аналіз цифрових доказів і методи тестування вразливості (фазинг, реверс-інжиніринг програмного забезпечення замків).

Ключові слова: *смартзамки; криміналістична експертиза; цифровий злам; фізичний злам; безпека; судова експертиза*

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

45 Білоус В. В., Шепітько В. Ю. Технічні засоби профілактики / В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін. Криміналістика : підручник. У 2 т. Т. 1 ; за ред. В. Ю. Шепітька. Харків, 2019. С. 57—63.

Participants

The author has contributed solely to intellectual discussion underlying this document, case law research, writing and editing, and assumes responsibility for its content and interpretation.

Declaration of Competing Interest

Author declares no conflict of interest.

References

2024 Consumer Cyber Readiness Report (2024) / Aspen Digital : website. URL: https://www.aspendigital.org/report/2024-consumer-cyber-readiness-report/.

Adaramola, O. O., Odigbo, Ch. S., Elelegwu, D., Chen, L. (2025). *Safeguarding Smart Homes: A Digital Security and Digital Forensics Approach* / ResearchGate : website. DOI: 10.13140/RG.2.2.19403.30240.

Ayers, R., Brothers, S., Jansen, W. (2014). *NIST Special Publication 800-101. Rev. 1. Guidelines on Mobile Device Forensics*. U. S. Department of Commerce ; NIST. DOI: 10.6028/NIST.SP.800-101r1.

Berrios, J., Mosher, E., Benzo, S., Grajeda, C., Baggili, I. (2023). Factorizing 2FA: Forensic analysis of two-factor authentication applications. *Forensic Science International: Digital Investigation*. Vol. 45. Suppl. Art. 301569. DOI: 10.1016/j.fsidi.2023.301569.

Bilous, V. V., Shepitko, V. Yu. (2019). Tekhnichni zasoby profilaktyky / V. Yu. Shepitko, V. A. Zhuravel, V. O. Konovalova ta in. *Kryminalistyka* [Criminalistics] : pidruchnyk. U 2 t. T. 1 ; za red. V. Yu. Shepitka. Kharkiv [in Ukrainian].

Black Hat USA 2019 (Mandalay Bay / Las Vegas) (2019) / Black Hat : website. URL: https://www.blackhat.com/us-19/.

Black Hat USA 2021 (Mandalay Bay / Las Vegas + Virtual) (2021) / Black Hat : website. URL: https://www.blackhat.com/us-21/.

Black Hat USA 2023 (Mandalay Bay / Las Vegas + Virtual) (2023) / Black Hat : website. URL: https://www.blackhat.com/us-23/.

Black Hat / DEF CON 2024: Latest Insights on Security and AI. ISMG Compendium Showcases More Than 50 Interviews on Threats, Emerging Solutions (2024) / Bank Info Security : website. URL: https://www.bankinfosecurity.com/black-hat-def-con-2024-latest-insights-on-security-ai-a-26283.

Caballero-Gil, C., Álvarez, R., Hernández-Goya, C., Molina-Gil, J. (2024). Research on smart-locks cybersecurity and vulnerabilities. *Wireless Networks*. Vol. 30. DOI: 10.1007/s11276-023-03376-8.

Cheremnova, A. I., Bielik, L. S. (2023). Tsyfrova informatsiia yak ob'iekt ekspertnoho doslidzhennia v umovakh didzhytalizatsii: problemy ta perspektyvy rozvytku [Digital Information as an Object of Expert Research in the Context of Digitalization: Problems and Development Prospects]. *Kryminalistyka i sudova ekspertyza*. Vyp. 68. DOI: 10.33994/kndise.2023.68.06 [in Ukrainian].

Cybersecurity Subteam Recommendations (2023) / National Institute of Standards and Technology : website. URL: https://surl.li/fkkmcm.

Dashevskyi, S., La Spina, F. (2023). Old Code Dies Hard: Finding New Vulnerabilities in Old Third-Party Software Components and the Importance of Having SBoM for IoT / OT Devices / *Black Hat Europe 2023*. URL: https://i.blackhat.com/EU-23/Presentations/EU-23-Dashevskyi-Old_code_dies_hard.pdf.

Dufeniuk, O. M. (2024). Maibutnie 3D kryminalistyky: innovatsii, yaki zminiuiut praktyku dosudovoho rozsliduvannia [The Future of 3d Forensic Science: Innovations That Change the Practice of Pre-Trial Investigation]. *Yurydychnyi naukovyi elektronnyi zhurnal.* № 3. DOI: 10.32782/2524-0374/2024-3/110 [in Ukrainian].

Federal Bureau of Investigation. Internet Crime Report 2023 (2023) / Internet Crime Complaint Center. URL: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf.

Four Ways 3D Printing May Threaten Security (2018) / RAND Corporation : website. URL: https://www.rand.org/pubs/articles/2018/four-ways-3d-printing-may-threaten-security.html.

Garland, L., Neyaz, A., Varol, C., & Shashidhar, N. K. (2024). Investigating Digital Forensic Artifacts Generated from 3D Printing Slicing Software: Windows and Linux Analysis. *Electronics*. 2024. Vol. 13 (14). DOI: 10.3390/electronics13142864.

Hill, G. (2014). *3-D Printed Skeleton Key Can Open Almost Any Lock in Seconds* / Security Today : website. URL: https://securitytoday.com/articles/2014/09/03/3d-printed-skeleton-key-can-open-almost-any-lock-in-seconds.aspx.

Hrabovskyi, H., Oparii, A., Kuznietsov, R. (2019). Osoblyvosti ekspertnoho doslidzhennia slidiv znariad zlomu [Features of Expert Research on Traces of Hacking Tools]. *Molodyi vchenyi*. № 8 (72). DOI: 10.32839/2304-5809/2019-8-72-61 [in Ukrainian].

Hutchinson, Sh., Yoon, Y. H., Shantaram, N., & Karabiyik, U. (2020). Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory. *2020 ASEE Virtual Annual Conference Content Access*. DOI: 10.18260/1-2--34868.

Kent, K., Chevalier, S., Grance, T., Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology. SP 800-86*. U. S. Department of Commerce ; Technology Administration ; NIST. URL: https://surl.gd/bfuxct.

Kerrison, S. (2022). IoT Droplocks: Wireless Fingerprint Theft Using Hacked Smart Locks. *ArXiv*. DOI: 10.48550/arXiv.2208.13343.

Kopcha, V. V., Fridmanskyi, R. M., Kopcha, N. V. (2022). Pravove doslidzhennia slidiv na mistsi zlochynu: yaki spryiaiut efektyvnomu rozkryttiu i poperedzhenniu zlochyniv [Legal investigation of crime trace tracks: facilitating effective detection and prevention of crimes]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo*. Vyp. 72. Ch. 2. DOI: 10.24144/2307-3322.2022.72.67 [in Ukrainian].

Kuznietsov, R. V., Yevsieiev, P. O. (2022). Osoblyvosti trasolohichnoho doslidzhennia dynamichnykh slidiv znariad zlamu [Features of tracelogical study of dynamic traces of breaking tools]. *Analitychno-porivnialne pravoznavstvo*. № 4. DOI: 10.24144/2788-6018.2022.04.61 [in Ukrainian].

Ollam, D. (2010). *Practical Lock Picking: A Physical Penetration Tester's Training Guide*. Syngress.

Osawa, Y., Higuchi, S. (2023). A Manufacturer's Post-Shipment Approach to Fend-Off IoT Malware in Home Appliances / *Black Hat USA 2023*. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf.

Santos, D. dos, Guiot, S., Dashevskyi, S., Amri, A., Kerro, O. (2023). Route to Bugs: Analyzing the Security of BGP Message Parsing / *Black Hat USA 2023*. URL: https://i.blackhat.com/BH-US-23/Presentations/US-23-dosSantos-Route-to-Bugs-Analyzing-the-Security-of-BGP.pdf.

Shepitko, V. Yu., Konovalova, V. O., Zhuravel, V. A. ta in. (2008). *Kryminalistyka* [Criminalistics] : pidruchnyk / za red. V. Yu. Shepitka. 4-te vyd., pererob. i dopov. Kharkiv. URL: https://law.sspu.edu.ua/files/documents/books/library/17/shepitko.pdf [in Ukrainian].

Smith, S. W., Oorschot, P. C. van. (2019). The Internet of Things: Security Challenges. *IEEE Security and Privacy Magazine*. Art. 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918.

Winkelmann, A. (2022). *Unauthorized Smart Lock Access. Ethical Hacking of Smart Lock Systems*. Stockholm, Sweden. URL: https://kth.diva-portal.org/smash/get/diva2%3A1749555/FULLTEXT01.pdf.

Yakymenko, R. V. (2018). Shchodo vazhlyvosti etapu porivnialnoho doslidzhennia konformnykh slidiv na detaliakh mekhanichnykh suvaldnykh zamkiv [On the Importance of the Stage of Comparative Study of Conformal Traces on the Details of Mechanical Lever Locks]. *Kryminalistyka i sudova ekspertyza.* Vyp. 63. Ch. 1. URL: https://digest.kndise.gov.ua/wp-content/uploads/2021/06/2018_1.pdf [in Ukrainian].

Pidnebennyi, R. (2025). Comparative Analysis of Smart Lock Breaching Methods and Their Forensic Examination in Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics.* Issue 1 (38). P. 182—199. DOI: 10.32353/khrife.1.2025.12.