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

Роман Піднебенний *

* LLC Undersky Locksmith, Нью-Йорк, США, e-mail: underskylock@gmail.com

DOI: 10.32353/khrife.1.2025.12 УДК 343.98(477+73)
Надійшло 28.02.2025 / Рецензовано 05.03.2025 / Прийнято до друку 26.03.2025 / Доступно онлайн 31.03.2025

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.*

Постановка наукової проблеми

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 [1]. Відсутність єдиного підходу до криміналістичної експертизи цих злочинів в Україні та США створює труднощі у правоохоронній діяльності, тож розв'язання цієї проблеми є актуальним у сучасному інноваційному світі.

Мета статті

Дослідити методи зламу смартзамків, порівняти особливості криміналістичних експертиз подібних зламів в Україні та США й запропонувати заходи для вдосконалення розслідування таких злочинів.

Методи дослідження

Застосовано метод порівняльного аналізу, трасологічний метод експертизи слідів зламу, аналіз цифрових доказів і методи тестування вразливості (фазинг, реверс-інжиніринг програмного забезпечення замків).

Аналіз основних досліджень і публікацій

Особливості експертного дослідження зламу механічних і смартзамків розглядали науковці як України (Р. Якименко [2], Г. Грабовський зі співавторами [3], Р. Кузнєцов та П. Євсєєв [4], В. Копча зі співавторами [5]), так і інших країн (*D. Ollam* [6], *S. Dashevskyi* та *F. La Spina* [7], *D. dos Santos* зі співавторами [8], *Y. Osawa* та *S. Higuchi* [9]).

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 (дата звернення: 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 (дата звернення: 01.02.2025).

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

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 (дата звернення: 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/

Викладення основного матеріалу дослідження

Із розвитком технологій збільшується кількість і вдосконалюється якість загроз, пов'язаних зі зламом замків як звичайних, так і високотехнологічних (зокрема, «розумних»).

У США значну увагу приділяють цифровій криміналістиці зламу смартзамків (приміром, у *National Forensic Science Technology Center*, далі — *NIST*[10]), тоді як в Україні поки переважає фізична експертиза зламу механічних елементів.

Популярні бренди смартзамків у США: *August, Yale, Schlage, Kwikset, Wyze*. В Україні більш поширені китайські моделі: *Xiaomi, Aqara*, дешеві *OEM*-рішення.

Методи автентифікації у США — біометрія, *PIN*-коди, *NFC, Bluetooth, Wi-Fi*[11], в Україні — *RFID*-картки, *PIN*-коди, механічні ключі.

Основні вразливості смартзамків у США: перехоплення бездротових сигналів, добирання кодів, атаки за допомогою мобільних застосунків [12]. Натомість в Україні загрози слід чекати через механічні злами, перебої в електропостачанні, застаріле програмне забезпечення.

Отже, оскільки методи зламу механічних і смартзамків у США й Україні певною мірою різняться, то різнитимуться також особливості експертного дослідження таких зламів, що ми докладно розглянемо далі.

Методи зламу замків та особливості їх дослідження у США

Варто зауважити, що смартзамки залишають унікальні сліди несанкціонованого доступу — докази, як-от:

- журнали доступу — збережені записи про відімкнення (замкнення) замка можуть містити інформацію про час зламу або спроби введення неправильного коду;
- дані про *Bluetooth*- або *Wi-Fi*-з'єднання — здатні надати відомості про хакерські інструменти для перехоплення або добирання коду доступу;
- форензичний аналіз мобільних застосунків — якщо замок контролюють за допомогою смартфона, можна відстежити взаємодію із застосунком, навіть якщо зловмисник спробував його видалити.

Смартзамки набули значного поширення завдяки зручності застосування

Presentations/US-23-Osawa-Higuchi-A-Manufacturers-Post-Shipment-Approach.pdf (дата звернення: 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 (дата звернення: 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 (дата звернення: 01.02.2025) ; Cybersecurity Subteam Recommendations / National Institute of Standards and Technology : website. 2023-08-18. 5 p. URL: https://surl.li/fkkmcm (дата звернення: 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 (дата звернення: 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 (дата звернення: 01.02.2025).

й інтегруванню із системами «розумного будинку» [13].

Згідно з дослідженням 2023 року, 12 % власників смартзамків у США зазнали спроб зламу їхніх пристроїв. Основні загрози:

- фізичний злам (43 %) — *3D*-друковані відмикачки, бампінг, магнітні маніпуляції;
- кібератаки (37 %) — злам мобільних застосунків, перехоплення бездротових сигналів через *Bluetooth* або *Wi-Fi*;
- атаки на систему автентифікації (20 %) — злам паролів або маніпуляції з *NFC*-картами [14].

У 2023 році *FBI IC3* отримав 2825 скарг на атаки програм-вимагачів, що спричинили збитків на понад $59,6 мільйона [15]. Подібні програми шифрують дані на пристрої, що робить їх недоступними для користувачів, а кіберзлочинці вимагають викуп за повернення викраденої інформації. Зафіксовано випадки, коли зловмисники атакували «розумні замки»: блокували доступ до приміщень, використовуючи це як інструмент вимагання викупу (наприклад, в австрійському готелі *Romantik Seehotel Jäegerwirt* хакери зламали систему електронних ключів, заблокували гостей у їхніх номерах і вимагали викуп для відновлення доступу). Це свідчить про вразливість *IoT*-пристроїв (від англ. *Internet of Things* — інтернет речей), зокрема, систем електронних замків, які можуть стати мішенню для атак, що порушує безпеку користувачів і завдає фінансових збитків. У *2024 Consumer Cyber Readiness Report* зазначено, що 7 % зареєстрованих кібератак у 2024 році пов'язані з атаками програм-вимагачів на «розумні пристрої» для дому (зокрема, «розумні замки») [16]. Учасники конференцій *Black Hat USA 2023* та *DEF CON* уже не вперше [17] розглядали нові методи атак на смартзамки (включно із застосуванням *3D*-друкованих відмикачок і магнітних маніпуляцій), засоби викриття, попередження та криміналістичного дослідження таких атак.

Із розвитком технологій змінюються як методи зламу, так і способи їх криміналістичного дослідження. Традиційні механічні замки залишають фізичні сліди зламу, тоді як смартзамки можуть містити цифрові сліди, дослідження яких потребує спеціального аналізу.

Серед методів зламу смартзамків у США особливо вирізняються цифрові атаки, що базуються на вразливості програмного забезпечення та мережевих

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 (дата звернення: 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 (дата звернення: 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 (дата звернення: 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/ (дата звернення: 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/ (дата звернення: 01.02.2025).

протоколів [18]. Аналіз зламу смартзамків у США ґрунтується на стандартизованих методиках цифрової криміналістики, які дають змогу правоохоронцям точно з'ясувати обставини зламу, виявити спосіб несанкціонованого доступу й ідентифікувати злочинця.

Так, наприклад, перехоплення *Bluetooth* і *Wi-Fi* застосовують для дешифрування переданих даних або клонування автентифікаційних ключів [19]. Виявлено також можливість перехоплювати й відтворювати *Bluetooth*-команди, що надали несанкціонований доступ до замка, без потреби у фізичному ключі. Більшість смартзамків послуговуються *Bluetooth Low Energy* (далі — *BLE*) або *Wi-Fi* для зв'язку зі смартфоном власника. Зловмисники можуть застосувати такі методи зламу:

- перехоплення *Bluetooth*-підключень — хакери можуть записати сеанс зв'язку та спробувати відтворити його для отримання доступу;
- атаки на *Wi-Fi*-з'єднання — якщо замок підключено до інтернету, можливі атаки для підміни команд, подібні до *Man-in-the-Middle*;
- брутфорс-атаки — добирання паролів або цифрових кодів за допомогою автоматизованих скриптів.

Існують і інші загрози, як-от:

- програмні атаки (*API*-вразливості) — експлуатація помилок у мобільних застосунках, що контролюють смартзамки [20]. Через слабку автентифікацію користувачів або із застосуванням спеціального обладнання зловмисники здатні віддалено перехопити контроль, сигнал між мобільним пристроєм і замком;
- несанкціоноване збирання біометричних даних — модифікований зловмисниками «розумний замок» зчитує відбитки пальців користувача та передає їх зашифрованими каналами на віддалений і контрольований сервер без відома власника такого замка;
- злам алгоритмів розпізнавання — за допомогою атак «відбиток-повторювач» застосовують перехоплені біометричні дані для отримання доступу до інших пристроїв власника.

Саме тому необхідно локально зберігати біометричні дані й послуговуватися надійними механізмами захисту, наприклад, шифруванням *FIDO2* (від англ. *Fast IDentity Online 2* — відкритий стандарт автентифікації користувачів, покликаний зміцнити процедуру входу користувачів до онлайнових служб для підвищення загальної довіри) [21].

Непоодинокі також випадки фізичного втручання в систему змішаних механізмів смартзамків (*3D*-друковані відмикачки, магнітні маніпуляції). У США *3D*-друкованими відмикачками активно

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 (дата звернення: 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 (дата звернення: 01.02.2025).

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

послуговуються дослідники в галузі фізичної безпеки і, на жаль, зловмисники у спробах обійти традиційні механічні захисти[22]. Основні способи застосування:

- дублікати ключів — *3D*-друк створює точні копії ключів лише за їхніми фотографіями або вимірами;
- шляхом зламу серцевини замка — надруковані відмикачки здатні легко відчиняти циліндрові механізми, які мають широкий попит;
- заміна традиційних відмикачок— сучасні матеріали *3D*-друку доволі міцні для маніпулювання механізмами замків.

Учасники конференції *Black Hat USA 2019* продемонстрували, як *3D*-друк можна застосувати для створення відмикачки, про які йшлося вище[23]: зокрема, *L. Garland* зі співавторами з'ясувала, що аналіз артефактів, згенерованих у процесі *3D*-друку, виявив наявність цифрових слідів на всіх досліджених етапах[24]. Ці артефакти можуть мати важливе значення для цифрової криміналістики, оскільки містять дані, пов'язані з *3D*-принтером, програмним забезпеченням для нарізки (англ. *slicing software*) і файлами *G-code*. Дослідження цифрових слідів *3D*-друку особливо актуальне в контексті безпеки, зокрема у разі виготовлення нелегальних інструментів для зламу замків. Як зазначила *G. Hill* (2014), *3D*-друковані ключі застосовують для відмикання складних замків за лічені секунди, що є серйозним викликом безпеці[25].

Захист від *3D*-друкованих відмикачок можливий: застосовувати запатентовані профілі ключів, які складніше скопіювати, багаторівневий механізм системи пінів, що ускладнює розблокування друкованими інструментами.

Фахівці з безпеки також спостерігають магнітне втручання в електромеханічні замки або традиційні моделі із застосуванням магнітних ключів, коли зловмисники користуються потужними неодимовими магнітами для переміщення механічних частин замка, маніпулюють електронними компонентами замка для подолання автентифікації та здійснюють реверс-інжиніринг магнітних ключів, що дає змогу створити аналог без фізичного контакту з оригіналом.

Сильні магніти здатні оминати електронні й механічні блокування. На *Black Hat USA 2021* підтвердили, що 54 % протестованих електронних замків вразливі до впливу магнітів, оскільки не мають відповідного екранування[26]. Методи захисту: застосування немагнітних сплавів у критичних частинах

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 (дата звернення: 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 (дата звернення: 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/ (дата звернення: 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 (дата звернення: 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 (дата звернення: 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/ (дата звернення: 01.02.2025).

замка; облаштування захисного корпусу від зовнішніх магнітних впливів; запровадження алгоритмів розпізнавання несанкціонованого оперування електронними замками.

Отже, *3D*-друковані відмикачки й магнітні маніпуляції — це реальні загрози для фізичної безпеки замків у США. Криміналістичний аналіз подібних злочинів тут зосереджено на виявленні залишкових слідів *3D*-відмикачок у механізмах замків та аналізі магнітного впливу.

Рішення для захисту: комбінування електронних і механічних методів захисту, застосування складніших профілів ключів і магнітостійких матеріалів.

Методи зламу замків та особливості їх дослідження в Україні

В Україні злам механічних замків залишається найпоширенішим видом злочинів, пов'язаних із несанкціонованим доступом (порівняно із цифровим зламом). Для механічних замків найбільш поширеними методами є бампінг, маніпулювання відмикачками, свердління та силовий злам, які залишають характерні сліди на деталях замка. Смартзамки, що набувають усе більшого поширення, зазнають як фізичних, так і цифрових атак, включно з перехопленням бездротових сигналів, експлуатуванням уразливості програмного забезпечення та зламом мобільних застосунків.

Р. Якименко докладно описав аналіз механічного зламу через конформні сліди на деталях замків — *бампінг*[27]. Це метод відкриття циліндрових замків без оригінального ключа із застосуванням спеціального бампключа, який устромляють у замкову щілину та піддають легким ударам, змушуючи піни замка підстрибувати, що дає змогу провернути циліндр і відімкнути замок. Криміналістичний аналіз бампінгу зосереджують на виявленні конформних слідів — характерних мікропошкоджень на внутрішніх компонентах замка, спричинених ударами бампключа (зокрема, мікроскопічних ум'ятин або подряпин на пінах і шпулерах; нерівномірного зношування або деформування на поверхні контактів).

Для детекції таких слідів застосовують високоточні мікроскопи й інші інструменти, які дають змогу ретельно оглянути внутрішні компоненти замка. Виявлення цих ознак є критично важливим для підтвердження факту несанкціонованого доступу за допомогою бампінгу, оскільки зовнішні пошкодження зазвичай відсутні. Додавання цього аналізу до криміналістичної експертизи допоможе правоохоронним органам ефективніше розслідувати випадки незаконного проникнення та сприятиме притягненню винних до відповідальності.

Застосування для зламу відмикачок і свердління розглянуто в підручнику «Криміналістика» за редакцією В. Шепітька[28]. *Відмикачки* — це набір спеціальних інструментів для маніпулювання внутрішніми механізмами замка без застосування оригінального ключа.

За призначенням відмикачки можна класифікувати так:

- ручні (спеціальні гачки, лопатки, натягувачі) дають змогу операторові індивідуально дібрати позицію штифтів у механізмі циліндрового замка;

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

- автоматизовані (електронні або ударні) працюють за принципом швидкого добирання комбінації без необхідності докладного маніпулювання.

Відмикачки залишають характерні конформні сліди на внутрішніх деталях замка, зокрема:

- подряпини й потертості на пінах і сувальдах — виникають через багаторазові маніпулювання;
- нерівномірне зношування механізму — нехарактерне пошкодження або зміна положення штифтів;
- зміни натягу пружин — через застосування силових методів маніпулювання.

Названі вище пошкодження є доказами у кримінальному розслідуванні, оскільки дають змогу визначити метод і знаряддя зламу, а також відрізнити застосування злочинцями спеціалізованих інструментів від стандартного зношування замка.

Свердління є одним з найбільш деструктивних методів зламу, що передбачає фізичне руйнування механізму секретності замка, даючи змогу відчинити його без оригінального ключа.

Типові точки свердління залежать від конструкції замка:

- свердління циліндра — знищення механізму штифтів у циліндрових замках;
- свердління поруч із ригелем — у сувальдних та електронно-механічних замках для примусового розблокування механізму.

Криміналістичний аналіз свердління:

- отвори від свердла — їхні діаметр, форма та розташування можуть надати інформацію про інструмент, яким здійснювали злам;
- металева стружка свідчить про характер і напрямок свердління, що сприятиме відтворенню дій злочинця;
- термічні пошкодження можуть виникати через застосування високошвидкісних дрилів або інструментів із підвищеним тертям.

Злочинці частіше застосовують свердління для зламу сейфів, електронно-механічних систем і високоміцних замків, оскільки це дає змогу швидко подолати складний механізм без потреби у високій майстерності, як у випадку з відмикачками.

Отже, механічний спосіб зламу в Україні є більш релевантним.

Аналіз механічних слідів зламу

Аналіз механічних слідів зламу є ключовим аспектом судової криміналістики, оскільки дає змогу:

- з'ясувати метод зламу — визначити, чи застосовували зловмисники відмикачки або силові методи, як-от свердління;
- ідентифікувати інструменти злочинців — характер пошкоджень може свідчити про конкретний тип відмикачок або свердла, що допомагає співвіднести їх із інструментами затриманих осіб;
- виявити рівень підготовки зловмисників — професійні злами часто залишають мінімальні пошкодження, тоді як аматорські — більш виражені;
- підтвердити або спростувати факт несанкціонованого проникнення — відсутність слідів зламу може означати інсценування.

Застосування сучасних технологій — *3D*-сканування мікропошкоджень і спектрального аналізу металевих частинок — дає змогу отримати більш точні дані для експертизи: розвиток

3D-криміналістики науковці вважають необхідним для сприяння практиці розслідування злочинів [29].

Отже, сьогодні в Україні трасологічне дослідження слідів, залишених знаряддями зламу, є ключовим етапом у криміналістичному аналізі злочинів, пов'язаних зі зламом замків. Основні типи слідів, які можна виявити на корпусі замка або в його механізмі:

- сліди деформації — ум'ятини, подряпини, вигини на металі корпусу або циліндра;
- динамічні сліди впливу — тертя або зсув у разі застосування важелів, викруток, лома або спеціальних відмикачок;
- мікроушкодження внутрішнього механізму — можливе свідчення маніпулятивного зламу за допомогою бампінгу або електронних методів впливу.

Згідно з дослідженням Г. Грабовського зі співавторами [30], трасологічний аналіз слідів зламу проводять із застосуванням оптичних мікроскопів і цифрових інструментів для з'ясування механізму утворення ушкоджень та типу знаряддя, яким здійснювали злам.

Щодо динамічних слідів зламу, то вони містять важливу інформацію для відтворення механізму зламу замка й визначення типу застосованого інструмента. Р. Кузнєцов і П. Євсєєв виокремлюють такі ключові параметри аналізу:

- глибина і форма подряпин — свідчить про тип знаряддя (лом, викрутка, молоток тощо);
- кут нахилу й напрямок руху слідів — допомагає з'ясувати механізм застосування сили;
- наявність залишків металу — може свідчити про контакт зі спеціальними інструментами зламу [31].

Комп'ютерне трасологічне моделювання дає змогу точно реконструювати злам і порівняти знайдені сліди з відомими видами знарядь, найчастіше застосовуваними у кримінальних діях.

Отже, дослідження слідів механічного зламу смартзамків є критично важливим для ідентифікації методів проникнення та знарядь зламу. Поєднання трасологічного аналізу, комп'ютерного моделювання і правового супроводу підвищує точність криміналістичних експертиз та ефективність розслідувань. Однак, на відміну від США, де швидкими темпами зростає попит на смартзамки, в Україні ці системи застосовують не настільки масово, а цифрові атаки на замки фіксують іще рідше. Водночас відсутність оновлень програмного забезпечення та слабкий рівень шифрування в поширених китайських моделях смартзамків створює серйозні ризики їхнього зламу.

Аналіз цифрових слідів зламу

Аналіз зламу смартзамків у США ґрунтується на стандартизованих методиках цифрової криміналістики, які дають змогу правоохоронцям точно визначити обставини зламу, виявити спосіб несанкціонованого доступу й ідентифікувати злочинця.

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 (дата звернення: 01.02.2025).

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

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

Сучасна криміналістика США розглядає цифрові сліди як повноцінний доказ, еквівалентний традиційним фізичним слідам (наприклад, відбиткам пальців або слідам інструментів зламу).

Основні принципи збору й аналізу цифрових доказів:

- цілісність (англ. *Integrity*) — доказ не можна змінювати або пошкоджувати під час вилучення;
- автентичність (англ. *Authenticity*) — необхідно довести, що отримані цифрові сліди дійсно належать до певного злочинного інциденту;
- відтворюваність (англ. *Reproducibility*) — незалежні експерти повинні мати змогу повторити аналіз і отримати аналогічні результати;
- ланцюжок збереження доказів (англ. *Chain of Custody*) — слід задокументувати, хто, коли та як отримував доступ до цифрових доказів.

Під час розслідування зламу смартзамків у США традиційні криміналістичні методи комбінують з методами цифрової криміналістики.

Сучасні смартзамки зберігають у журналі подій інформацію про таке:

- дату й час кожного відмикання / замикання;
- спроби введення неправильного коду або підключення невідомого пристрою;
- перезапуски системи або зміну паролів доступу.

Правоохоронці можуть отримати таку інформацію безпосередньо із замка або із серверів виробника. У США існує прецедентне право, що дає змогу отримати ці дані через судовий запит відповідно до *Stored Communications Act* (*SCA*, 1986), який регулює доступ до електронних комунікацій.

Методи аналізу журналів:

- форензичне копіювання (англ. *Forensic Imaging*) — створюють точну копію журналу подій для подальшого аналізу без зміни оригінальних даних;
- хронологічний аналіз (англ. *Timeline Analysis*) — вивчають послідовність подій для виявлення підозрілих дій (наприклад, спроб входу в незвичний час або з невідомого пристрою);
- кореляція з іншими джерелами (англ. *Correlation with Other Sources*) — порівнюють дані із замка з логами *Wi-Fi*-роутера, записами камер спостереження та даними мобільних операторів.

Більшість смартзамків зв'язуються зі смартфоном власника за допомогою *BLE* або *Wi-Fi*. У разі зламу застосовують такі методи криміналістичного аналізу:

- аналіз радіочастотного трафіку — застосування спеціальних пристроїв (наприклад, *Wireshark* або *HackRF*) для перехоплення сигналів;
- форензичний аналіз маршрутизатора — вивчення логів *Wi-Fi*-підключень дає змогу з'ясувати, чи застосовували для зламу невідомий пристрій;
- відновлення *Bluetooth*-логів — за допомогою програмного забезпечення (наприклад, *BLE Sniffer*) можна проаналізувати історію підключень.

Смартзамками керують за допомогою мобільного застосунку, який може містити цінну інформацію про послуговування пристроєм і потенційний злам. У США для вилучення й аналізу даних з мобільного пристрою застосовують, зокрема, *Cellebrite UFED* — професійне програмне забезпечення для вилучення даних зі смартфонів, *Magnet AXIOM* дає

змогу аналізувати журнали дій у мобільному застосунку замка.

Autopsy (*The Sleuth Kit*) — відкритий інструмент для аналізу даних смартфонів. Методи аналізу:

- декодування логфайлів мобільного застосунку — витягають інформацію про спроби авторизації, помилки з'єднання, скидання пароля тощо;
- перевірка кешованих даних — навіть після видалення програми деякі дані можуть залишатися у пам'яті пристрою;
- кореляція із *GPS*-даними — дає змогу визначити, чи був власник замка в момент зламу поруч з об'єктом, чи замок зламано дистанційно.

Багато смартзамків синхронізують свої дані із сервером виробника, що дає змогу отримати додаткові цифрові сліди. Журнали активності користувача записують усі зміни в системі безпеки. Історія оновлень програмного забезпечення може показати, чи застосовували відомий експлойт для зламу. Якщо замок зламано віддалено, на сервері можуть залишитися цифрові сліди атаки — *IP*-адреси зловмисників. Правоохоронні органи США можуть отримати доступ до цих даних на підставі *Stored Communications Act*, подавши запит до компанії-виробника. Методи аналізу серверних даних:

- журнали доступу — переглядають записи входу та спроби змінити налаштування;
- перевірка мережевих запитів — виявляють невідомі *IP*-адреси або підозрілі запити до *API* замка;
- форензичний аналіз *SQL*-баз — відновлення історії користування замком.

Підіб'ємо проміжні підсумки. У США для аналізу зламу смартзамка застосовують комплексний підхід — сукупність методів цифрової криміналістики: аналіз журналів, підключень, мобільного застосунку та серверних даних. Там вироблено чітку правову базу — закони, які регулюють отримання і застосування цифрових доказів у кримінальних провадженнях. До того ж правоохоронці мають доступ до необхідного технологічного оснащення — професійного обладнання та програмного забезпечення для аналізу зламу. Україна наразі не має подібної методичної бази, що значно ускладнює ефективний аналіз цифрових зламів. Тож для ефективної боротьби із цифровими зламами в Україні необхідно адаптувати кращі практики цифрової криміналістики США та запровадити відповідні правові механізми на законодавчому рівні.

Проблеми аналізу зламу смартзамків в Україні порівняно зі США

Зважаючи на викладене вище, виокремимо проблеми аналізу зламу смартзамків в Україні порівняно зі США:

- *обмежена спеціалізація експертів.* У США злам смартзамків аналізують не лише традиційні криміналісти, а й фахівці із цифрової безпеки, етичні хакери й експерти з *IoT*. В Україні ж ця галузь лише розвивається, і кількість експертів, здатних провести повноцінний аналіз цифрових слідів, залишається обмеженою;
- *відсутність уніфікованих методик цифрової криміналістики.* В американській практиці існують стандартизовані методики аналізу цифрових доказів (наприклад, рекомендації *NIST*). Україна, хоча й запроваджує окремі міжнародні напрацювання, усе ще не має уніфікованих підходів до аналізу

кіберзлочинів, зокрема, до методів дослідження зламу смартзамків;

- *обмежений доступ до спеціалізованого обладнання*. У США слідчі мають доступ до передових інструментів аналізу цифрових пристроїв (логічних аналізаторів, програмного забезпечення для вилучення даних та ін.) і спеціалізовані криміналістичні лабораторії. В Україні таких ресурсів значно менше, що ускладнює аналіз зламу сучасних електронних замків;
- *недостатня законодавча база для аналізу цифрових слідів*. У США аналіз цифрових слідів регламентовано законами, що дає змогу застосовувати здобуті дані в суді як доказ. Основні нормативні акти регулюють як методи зламу, так і відповідальність за несанкціонований доступ до *IoT*-пристроїв, включно з електронними замками.

Деякі зі згаданих вище нормативних актів США:

- *Federal Rules of Evidence* (1975) — обумовлює, що цифрові дані, включно з журналами входу смартзамків, мережеві логи та цифрові сліди зламу, є допустимими доказами в судових процесах;
- *Computer Fraud and Abuse Act* (*CFAA*, 1986, оновлений 2023 р.) — криміналізує несанкціонований доступ до комп'ютерних систем, включно зі спробами зламу *IoT*-пристроїв;
- *Electronic Communications Privacy Act* (*ECPA*, 1986, оновлений 2018 р.) — регулює порядок доступу правоохоронців до електронних комунікацій і хмарних серверів, на яких можуть зберігатися дані смартзамків;
- *Cybersecurity Information Sharing Act* (*CISA*, 2015) — передбачає обмін інформацією про кіберзагрози між державними установами й компаніями, що може бути застосовано для аналізу атак на смартзамки;
- *Federal Trade Commission Act* (*FTC Act*, 1914, оновлений 2021 р.) — дає змогу розслідувати випадки, коли виробники смартзамків не забезпечили належного рівня захисту своїх пристроїв, що спричинило злами або витік даних користувачів;
- *California Consumer Privacy Act* (*CCPA*, 2018) — регулює застосування та зберігання персональних даних, включно з інформацією, яку збирають смартзамки (біометричні дані, журнали доступу тощо).

Сукупність цих нормативних актів формує юридичне підґрунтя для розслідування злочинів, пов'язаних зі зламом смартзамків у США.

В Україні юридичні аспекти застосування електронних доказів у кримінальних справах до сьогодні перебувають у зародковому стані, унаслідок чого суди можуть не приймати такі докази через відсутність чіткої процедури їх фіксування та збереження. Саме тому аналіз цифрових слідів досі залишається проблематичним[32] через низку чинників, а саме:

- Кримінальний процесуальний кодекс України[33] (далі — *КПК*

32 Черемнова А. І., Бєлік 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 (дата звернення: 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 (дата звернення: 06.01.2025).

України) не містить чіткого визначення електронних доказів у кримінальних провадженнях. Це створює правову невизначеність щодо того, як правильно збирати та застосовувати цифрові докази, отримані зі смартзамків;

- відсутність уніфікованих стандартів аналізу цифрових слідів. Якщо у США існують затверджені методики *NIST*, то в Україні аналогічні стандарти тільки розробляють;
- обмежений доступ до логів і даних смартзамків. Наприклад, якщо виробник замка розташований за кордоном (що трапляється доволі часто), українським слідчим складно отримати журнали входу-виходу користувача;
- недостатня технічна база. В Україні лише кілька криміналістичних лабораторій мають сучасне програмне забезпечення для аналізу цифрових пристроїв;
- суди часто не приймають цифрових доказів через їх неправильне документування або відсутність відповідної експертизи.

На нашу думку, імплементація принципів *Berkeley Protocol* [34] в українську практику могла б сприяти стандартизації процесів роботи з електронними доказами. Це передбачає забезпечення достовірності й цілісності цифрових даних, що є критично важливим під час розслідування кіберзлочинів, зокрема, зламів смартзамків. Утім, для ефективного застосування цих принципів необхідно внести відповідні зміни до КПК України, де чітко визначити поняття «електронні докази» і процедури їх опрацювання [35].

На відміну від США, в Україні також значно більше випадків застосування дешевих або нелегально ввезених смартзамків без необхідних протоколів захисту. Це робить їх більш вразливими до зламу й водночас ускладнює їхню експертизу, оскільки відсутня офіційна документація, а виробник не співпрацює з правоохоронними органами.

Одним із ключових ризиків для безпеки смартзамків є застосування застарілих сторонніх програмних компонентів, які можуть містити невиявлені вразливості. Згідно з дослідженням *S. Dashevskyi* та *F. La Spina*, у багатьох *IoT*-пристроях застосовано компоненти, які не оновлювали роками, що відкриває набагато більше можливостей для атак зловмисників [36].

У дослідженні пристроїв *Sierra Wireless AirLink* виявлено 21 нову вразливість, із яких 15 стосувалися сторонніх програмних бібліотек. Це підтверджує необхідність регулярного аудиту програмного забезпечення та підтримання актуального *Software Bill of Materials* (далі — *SBoM*) [37].

Аналіз методів зламу смартзамків потребує комплексного підходу — урахування криміналістичних, кібербезпекових і правових аспектів. У США цей процес уже добре налагоджений завдяки

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 (дата звернення: 01.02.2025).

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

37 Ibid.

співпраці між правоохоронними органами, кіберекспертами й індустрією безпеки. В Україні ж криміналістична експертиза смартзамків стикається з низкою проблем, зокрема, нестачею кадрів, методичних стандартів, технічних можливостей і законодавчих механізмів. Для покращення ситуації необхідно поглиблювати навчання експертів, адаптувати міжнародні методики та вдосконалювати нормативну базу із цифрової криміналістики.

Для ефективного виявлення вразливостей у програмному забезпеченні *IoT*-пристроїв, включно зі смартзамками, дослідники застосовують фазинг-тестування. Як зазначають *D. dos Santos* зі співавторами, цей метод дає змогу знаходити слабкі місця у реалізаціях апаратних і мережевих протоколів, що також можна застосувати для аналізу безпеки смартзамків [38].

Фазинг дає змогу автоматично генерувати тисячі некоректних запитів, що допомагає виявляти критичні вразливості у програмному забезпеченні замків ще на етапі розробляння.

Інший підхід до підвищення безпеки *IoT*-пристроїв представлено в дослідженні *Y. Osawa* та *S. Higuchi*, де описано систему *ASTIRA* (інтелектуальна платформа), яку застосовують для збору й аналізу атак на *IoT*-пристрої, зокрема смартзамки [39].

Основні заходи для підвищення безпеки смартзамків:

- застосування *honeypots* — спеціально налаштованих пристроїв із вразливістю, своєрідних приманок для збору інформації про атаки;
- автоматизований аналіз шкідливого програмного забезпечення, що дасть змогу виявляти нові загрози на ранніх етапах;
- створення централізованої бази даних атак на *IoT*-пристрої, що допоможе виробникам швидше реагувати на нові загрози.

За даними дослідників, за останні 5 років зафіксовано понад 2,2 мільярди атак на *IoT*-пристрої, що свідчить про необхідність постійного моніторингу безпеки смартзамків [40].

Зважаючи на наведену вище інформацію, виокремимо кілька ключових рекомендацій для підвищення безпеки смартзамків:

- регулярний аудит програмного забезпечення — перевірка всіх сторонніх компонентів на наявність вразливості [41];
- запровадження фазинг-тестування під час розроблення смартзамків для виявлення потенційних слабких місць [42];
- застосування системи моніторингу атак на *IoT*-пристрої (таких, як

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 (дата звернення: 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 (дата звернення: 01.02.2025).

40 Ibid.

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

ASTIRA) для виявлення й аналізу загроз [43];
- забезпечення підтримки *SBoM* — документування всіх програмних компонентів для швидкого оновлення вразливих бібліотек [44].

Аналіз програмної вразливості смартзамків має важливе значення для криміналістичних розслідувань злочинів, пов'язаних зі зламом електронних систем доступу. Застосування фазинг-тестування дає змогу не лише виробникам підвищувати безпеку пристроїв, а й криміналістам відтворювати можливі сценарії зламу та виявляти застосовані злочинцями експлойти. Системи моніторингу атак (такі, як *ASTIRA*) дають змогу фіксувати спроби зламу в реальному часі, що може стати доказом у кримінальній справі. Створення централізованої бази даних атак на *IoT*-пристрої допомагає експертам ідентифікувати типові методи зламу й пов'язати окремі злочини один з одним. Окрім того, аналіз логів доступу та цифрових слідів, залишених вразливими смартзамками, є ключовим доказом у судових процесах. Отже, запровадження методів виявлення й усунення вразливості підвищує ефективність криміналістичної експертизи та допомагає правоохоронним органам у розслідуванні злочинів, пов'язаних із цифровими зламами.

У сучасній криміналістиці технічні засоби профілактики відіграють важливу роль у запобіганні злочинам і збиранні доказової інформації. До таких засобів належать охоронні системи відеоспостереження, електронні контролери доступу й хімічні маркери. Їх застосування не лише ускладнює скоєння злочинів, а й сприяє залишенню додаткових слідів під час спроби зловмисників нейтралізувати ці засоби. Своєю чергою це збільшує обсяг доказової інформації, доступної для слідства. Наприклад, під час взаємодії зі складними системами захисту злочинець може залишити на місці події сліди, які допоможуть ідентифікувати його особу або знаряддя зламу. Отже, запровадження сучасних технічних засобів профілактики не лише підвищує рівень безпеки, а й покращує ефективність криміналістичних досліджень [45].

Висновки

Попит на смартзамки у США й Україні збільшується з року в рік, однак водночас збільшується і кількість спроб їх зламати. Аналіз методів атак свідчить, що у США частіше застосовують цифрові атаки, тоді як в Україні домінують фізичні маніпуляції. Смартзамки є вразливими як до механічного, так і до цифрового зламу. Запровадження фазинг-тестування та застосування *honeypots* підвищить безпеку смартзамків. Захист смартзамків має поєднувати фізичні й цифрові заходи безпеки, що мінімізує ризики зламу та підвищить ефективність розслідування таких злочинів. Для аналізу атак на смартзамки також стануть у пригоді штучний інтелект, створення єдиної бази логів підключень смартзамків, розвиток цифрової криміналістики, поглиблене навчання спеціалістів,

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 (дата звернення: 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 (дата звернення: 01.02.2025).

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.

імплементація в національне законодавство американських стандартів судової експертизи.

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

Roman Pidnebennyi

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.*

Фінансування

Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності

Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники

Автор зробив свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і бере на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів

Автор заявляє, що у нього відсутній конфлікт інтересів.

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-hatdef-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].

Піднебенний, Р. (2025). Порівняльний аналіз методів зламу смартзамків і їхньої криміналістичної експертизи в Україні та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (38). С. 182—199. DOI: 10.32353/khrife.1.2025.12.