УДК 343.98:004.9:343.344
DOI: https://doi.org/10.31359/2079-6242-2025-50-184

Д. О. Чекін, доктор філософії з права, науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України
ORCID 0000-0002-9893-1588

МЕТОДИ І ЗАСОБИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ У БОРОТЬБІ З НЕЗАКОННИМ ЗАВОЛОДІННЯМ ТРАНСПОРТНИМИ ЗАСОБАМИ*

Постановка проблеми. У XXI столітті науково-технічний прогрес пов'язується зі стрімкими темпами розвитку цифрових та інформаційно-комунікаційних технологій і робототехніки. Ці маркери науково-технічного прогресу, що є результатом накопичення знань та удосконалення існуючих технологій, революціонізують транспортну галузь, оснащуючи автомобілі все більш складними системами, включаючи автоматичні системи керування та інтелектуальні асистенти водія. Проте розвиток технологічних рішень, асоціюючись насамперед із комфортними умовами існування, водночас «обтяжується» потенційними ризиками і негативними наслідками, оскільки його досягнення можуть бути «пристосовані» людиною під протиправні цілі[1].

Незаконне заволодіння транспортними засобами у сучасних умовах є яскравим проявом цього парадоксу. Злочинці використовують спеціалізовані технічні засоби, наприклад, телекомунікаційні комплекси «кодграбер[2]-ретранслятор». У зв'язку з цим діяння часто кваліфікуються як несанкціоноване втручання в роботу електронно-обчислювальних машин, що підтверджується актуальною судовою практикою[3].

Сучасні автомобілі обладнуються виробниками новітніми системами контролю доступу, які працюють за бездротовими технологіями, зокрема безключовим доступом, управління системами безпеки автомобіля через мобільні застосунки тощо. Проте іноді такі системи компрометуються зловмисниками, що дозволяє за наявності навичок програмування або користування спеціальними приладами перехоплювати зашифровані сигнали обміну даними систем безпеки та отримувати доступ не лише до салону автомобіля, а й навіть віддалено вмикати двигун.

З огляду на це цифрова криміналістика повинна адаптувати свої методи і засоби для виявлення та фіксації цифрових слідів протиправної діяльності, які знаходяться не лише у вбудованих системах автомобіля, а й у зовнішніх динамічних джерелах – хмарних серверах виробників[4]. Важливим завданням залишається забезпечення доказової цінності, автентичності та цілісності цих слідів у кримінальному провадженні.

Аналіз останніх досліджень і публікацій. Проблема заволодіння транспортними засобами є предметом ґрунтовного дослідження в Україні, свою увагу проблематиці приділяли як українські (А. Данилевський, С. Власенко, О. Федосова, О. Соломатіна), так і зарубіжні (M. Hargreaves,

* Примітка. Стаття підготовлена у межах розробки фундаментальної теми дослідження «Пріоритезація та технологізація у кримінальному провадженні у воєнний та повоєнний час» (держ. реєстр. в УкрІНТЕІ № 0124U005212).

[1] Батиргареєва В. С. 'Науково-технічний прогрес і правопорушення у сфері безпеки дорожнього руху та експлуатації транспорту: окремі ракурси проблеми' (2024) 48 Питання боротьби зі злочинністю 103–115. DOI: 10.31359/2079-6242-2024-48-103.

[2] *Примітка:* кодграббер – електронний пристрій, призначений для злому автомобільних сигналізацій шляхом перехоплення та підміни сигналу між брелоком та блоком керування, що дозволяє зловмиснику знешкодити охоронну систему та відкрити автомобіль.

[3] Постанова Верховного Суду від 02.10.2025 у справі № 523/503/20 (провадження № 12019160490003587) // Єдиний державний реєстр судових рішень. <URL: https://reyestr.court.gov.ua/Review/130683584> (дата звернення: 10.11.2025)

[4] Ebbers S. 'Grand theft API: A forensic analysis of vehicle cloud data' *Forensic Science International: Digital Investigation* (2024) DOI: https://doi.org/10.1016/j.fsidi.2023.301691

V. Harinam, B. Ariel) вчені. З публікацій авторів вбачається, що вчинення злочинів у сфері заволодіння транспортними засобами залишається розповсюдженим явищем незалежно від географії та соціально-економічного розвитку, хоча й мають певні особливості з урахуванням вказаних параметрів.

Питання виявлення, фіксації, вилучення та дослідження цифрових слідів у кримінальному провадженні у своїх працях досліджували Г. К. Авдєєва, М. В. Капустіна, А. В. Коваленко, І. А. Колеснікова, О. І. Крицька, К. В. Латиш, Р. Л. Степанюк, С. В. Стороженко, І. А. Тітко, В. М. Шевчук, В. Ю. Шепітько та інші науковці. Однак проблемам боротьби з незаконним заволодінням транспортними засобами з використанням можливостей цифрової криміналістики науковці приділяють недостатньо уваги.

Мета статті полягає в тому, щоб на основі матеріалів узагальнення шести судових справ, які розглядалися судами України різної юрисдикції, встановити типові сучасні способи і засоби, які використовують злочинці для незаконного заволодіння транспортними засобами, проаналізувати ключові методи та засоби цифрової криміналістики для ефективного розслідування незаконного заволодіння транспортними засобами, а також розробити практичні рекомендації для всіх зацікавлених сторін (науковців, правоохоронців і судових експертів) щодо мінімізації ризиків маніпуляції та забезпечення форензичної надійності, автентичності та цілісності цифрових слідів, отриманих із вбудованих та хмарних систем автомобілів, особливо в контексті технологізації у кримінальному провадженні.

Виклад основного матеріалу. Цифрова криміналістика сьогодні розглядається як комплексний напрям, що включає, окрім дослідження матеріальних пристроїв, також аналіз даних із хмарних сховищ електронно-обчислювальних машин та інформації, доступної через мобільні додатки-помічники[1]. Зростання модульності у виробництві, яке раніше детально не розглядалося науковцями, також збільшує ризики, що потребує окремого наукового пошуку[2].

Ключовим технічним методом для отримання даних є API-орієнтоване[3] отримання хмарних даних. Водночас існують загрози, пов'язані з витоком конфіденційної інформації через побічні канали, наприклад, відстеження активності мобільних пристроїв під час заряджання, навіть без проникнення в канали зв'язку, а тільки під час споживання пристроєм електроенергії[4].

Судова практика підтверджує, що незаконне заволодіння транспортними засобами (ч. 2 ст. 289 КК України) часто вчиняється із застосуванням спеціальних приладів. У справах, розглянутих Апеляційним судом м. Києва та Верховним Судом, фігурувало використання «Код-Грабера» для сканування автосигналізації та методу «провороту» для запуску автомобілів[5]. У справі № 646/110/17 було вилучено та досліджено пристрій із шістьма антенами та «глушилку» (пригнічувач частот)[6]. Верховний Суд у справі № 523/503/20 підтвердив, що використання кодграбера-ретранслятора є несанкціонованим втручанням в електронно-обчислювальні машини (ч. 2 ст. 361 КК України)[7].

Теоретично, криміналістичні дослідження мають спиратися на концепцію цифрового сліду, що є відображенням діяльності особи у матеріальному оцифрованому середовищі[8].

Аналіз сучасних методів злочину та технологій систем захисту транспортних засобів виявляє, що найбільшою проблемою є недосконалість або відсутність захищеного від втручання сховища да-

[1] –

[2] Голіна В. В. 'Вплив зарубіжних практик забезпечення безпеки дорожнього руху на концепції запобігання транспортним правопорушенням в Україні' (2024) 47 Питання боротьби зі злочинністю 124–132 DOI: 10.31359/2079-6242-2024-47-124

[3] *Примітка:* «API-орієнтоване» означає підхід до розробки програмного забезпечення, коли спочатку створюються API (Application Programming Interface – інтерфейси прикладного програмування), які дозволяють різним частинам програм взаємодіяти між собою та використовувати функціональність одна одної.

[4] Yang Q. 'On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel' (2017) 12 (5) IEEE Transactions on Information Forensics and Security. 1056–1066 DOI: 10.1109/TIFS.2016.2639446

[5] Ухвала Апеляційного суду м. Києва від 08.08.2018 у справі № 755/13969/16-к (провадження № 12016100040004640) URL: https://reyestr.court.gov.ua/Review/75970298 (дата звернення: 02.12.2025).

[6] Ухвала Полтавського апеляційного суду від 13.09.2022 у справі № 646/110/17 (провадження № 12016220060000877) URL: https://reyestr.court.gov.ua/Review/106413158 (дата звернення: 02.12.2025)

[7] Постанова Верховного Суду від 02.10.2025 у справі № 523/503/20 (провадження № 12019160490003587) // URL: https://reyestr.court.gov.ua/Review/130683584 (дата звернення: 02.12.2025)

[8] Meteňko J., Meteňková M. Digital trace as a personal and criminalistics object (2024) 9 (1) Security Horizons. 2024. DOI: 10.35603/sws.iscss.2024/s02/12

них у сучасних автомобілях. Ця критична вразливість дозволяє компетентним зловмисникам маніпулювати інформацією, знижуючи її доказову цінність. Крім того, важливою залишається проблема забезпечення прозорості та відтворюваності методів вилучення даних, особливо під час використання API-орієнтованих інструментів для отримання відповідної інформації із хмарних джерел. У зв'язку із цим необхідно розробити чіткі стандарти розширеного логування[1] та гарантувати захист інформації про походження доказів, що забезпечуватиме дотримання форензичної надійності доказів[2].

1. Способи та типові засоби незаконного заволодіння транспортними засобами.

Незаконне заволодіння транспортним засобом часто має корисливий мотив. Досить розповсюдженим є вчинення злочину за попередньою змовою групою осіб. Судова практика підтвердила можливість кваліфікації таких дій додатково за ч. 2 ст. 361 КК України (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж).

Проаналізовані судові кейси чітко ілюструють, що злочини, пов'язані з незаконним заволодінням транспортними засобами, давно вийшли за рамки традиційного фізичного зламу, перетворившись на високотехнологічну кримінальну діяльність, що вимагає застосування спеціальних знань і цифрових пристроїв. Це прямо корелює з потребою технологізації розслідування правопорушень, пов'язаних з незаконним заволодінням транспортними засобами.

Дослідження судової практики розгляду справ, пов'язаних із незаконним заволодінням транспортними засобами, дає зрозуміти, що типовими засобами, які застосовувалися злочинцями, є: телекомунікаційний комплекс «кодграбер-ретранслятор»; поєднання кодграбера та «методу провороту»; спеціалізовані пристрої «глушилки»; перепрограмований автомобільний комп'ютер та ін.

Випадок, розглянутий Верховним Судом у справі № 523/503/20, є знаковим для визначення правової природи сучасного угону. Обвинувачений разом із невстановленою особою придбав телекомунікаційний комплекс «кодграбер-ретранслятор», який складався з передавача і приймача, кустарним способом вмонтованих у корпуси побутової електроніки (відеопрогравача та телевізійної приставки). Механізм вчинення злочину полягав у тому, що шляхом використання цього комплексу було отримано доступ до салону, систем управління та двигуна автомобіля «Hyundai Santa Fe» Це, на думку суду, призвело до порушення встановленого порядку маршрутизації інформації. Саме цей аспект – порушення порядку маршрутизації інформації – дозволив судам кваліфікувати дії, спрямовані на електронний злом автомобіля, не лише за ч. 2 ст. 289 КК України (незаконне заволодіння), а й за ч. 2 ст. 361 КК України (несанкціоноване втручання в роботу ЕОМ). Таким чином, Верховний Суд визначив втручання у цифрові системи транспортного засобу як кіберзлочин.

Варто також зазначити, що у судовій справі № 755/13969/16-к фігурувало використання кодграбера для сканування автосигналізації та фізичного пристрою «провороту» для пошкодження замка запалення і запуску двигуна. Ця комбінація вказує на перехідний етап: від використання цифрового інструменту (кодграбера) для отримання доступу до подальшого застосування традиційних криміналістичних інструментів (провороту) для механічного заволодіння.

Випадок, розглянутий ухвалою Полтавського апеляційного суду у справі № 646/110/17, виявив застосування злочинцями спеціалізованих контрзасобів для запобігання викриттю та відстеженню. Обвинувачений був засуджений за замах на заволодіння транспортним засобом «Toyota Land Cruiser». Серед вилучених речових доказів фігурував пристрій, відомий як «глушилка». Експертне дослідження підтвердило, що цей пристрій був призначений для пригнічення сигналів CDMA/GSM, GPS, WIFI-частот, тобто для блокування мобільного зв'язку та GPS-трекерів, які можуть бути встановлені власником. На момент огляду всі тумблери пристрою були у ввімкненому положенні.

[1] *Примітка:* логування – процес запису подій, дій та стану програми чи комп'ютерної системи під час її роботи. Ця інформація фіксується у вигляді «бортових журналів» (логів), які допомагають розробникам аналізувати помилки, відстежувати поведінку системи та швидше їх усувати.

[2] Fröwis M. et al. 'Safeguarding the evidential value of forensic cryptocurrency investigations' (2020) 33 Forensic Science International: Digital Investigation Art. 200902. DOI: https://doi.org/10.1016/j.fsidi.2019.200902

Цей факт є надзвичайно важливим для цифрової криміналістики, оскільки він підтверджує, що злочинці активно технологізують процес приховування і знищення цифрових слідів. Використання «глушилок» унеможливлює відстеження викраденого транспортного засобу через GPS, що вимагає від правоохоронних органів автоматизації процесів збирання доказів шляхом аналізу інформації, яка міститься у вилученій у злочинців техніці («глушилка» та кодграбер) і досліджується в межах комп'ютерно-технічної експертизи.

Інші судові рішення підкреслюють пряму залежність угону від маніпуляцій внутрішніми електронними системами автомобіля:

1. Справа № 754/13878/17 (Київський апеляційний суд): злочинці для заволодіння автомобілями «Mitsubishi Lancer» та «Mazda-6» використовували не лише кодграбер для відкриття дверей і зняття з сигналізації, а й заздалегідь заготовлені так званий програматор автомобільних ключів, металевий ключ та електронний чіп для приведення в дію двигуна. Це свідчить про глибоке розуміння злочинцями архітектури безпеки транспортних засобів та здатність створювати нові ключі доступу.

2. Справа № 754/5026/20 (Київський апеляційний суд): Для незаконного заволодіння автомобілями «ВАЗ», «Hyundai Accent» та «Skoda Octavia» злочинці систематично використовували перепрограмований автомобільний комп'ютер та заготовку ключа. Як встановлено судом, особа, матеріали щодо якої виділені в окреме провадження, приєднувала перепрограмований комп'ютер до автомобіля, запускаючи двигун, тоді як обвинувачений виконував роль спостерігача.

Використання перепрограмованого автомобільного комп'ютера є квінтесенцією технологізації угону. Така «практика» – вже не просто обхід сигналізації, а пряма маніпуляція програмним забезпеченням вбудованих електронних блоків керування автомобіля, що замінює заводські налаштування і дозволяє ініціювати роботу двигуна без оригінального ключа. Це обґрунтовує наукове твердження про вразливість систем безпеки автомобілів, пов'язану з відсутністю або недосконалістю захищеного від втручання сховища даних у транспортних засобах, оскільки несанкціоноване втручання в електронну складову автомобіля стає типовим способом злочину. Крім того, наведені обставини підтверджують важливість роботи над методиками збору та дослідження цифрових доказів у вказаних категоріях справ.

2. Методи вилучення та аналізу цифрових слідів.

З огляду на те, що сучасний автомобіль функціонує як складна електронно-обчислювальна машина, яка постійно генерує та обмінюється даними, ефективне вилучення та дослідження цифрових слідів вимагає інтеграції методів, що охоплюють усі цифрові джерела: від внутрішніх блоків керування автомобілем до віддалених хмарних серверів. Цей комплексний підхід є ключовим для доведення стороннього втручання в роботу систем контролю за доступом до автомобіля.

Ефективність розслідування злочинів, пов'язаних із незаконним заволодінням автотранспортом, залежить від комплексного дослідження із застосуванням методів і засобів цифрової криміналістики усіх цифрових пристроїв автомобіля. При цьому вкрай важливим є дослідження електронної частини систем безпеки автомобіля, оскільки вони зберігають дані про історію відкривання / блокування дверей автомобіля, запуски двигуна та можуть фіксувати дані про історію його використання (швидкість, дистанція, час в дорозі, поточна геопозиція та маршрути переміщення). Під час виявлення автомобіля, який перебуває у розшуку як об'єкт протиправного заволодіння, криміналісту слідчо-оперативної групи є доцільним зняти (скопіювати) всю наявну інформацію з електронного блоку управління двигуном через діагностичні інтерфейси (OBD) та долучити електронний носій із копією такої інформації до протоколу огляду місця події. У випадку несанкціонованого доступу до транспортного засобу зловмисником така інформація стане доказом компрометації оригінального засобу доступу (ключа, картки, мобільного додатку), передбаченого виробником.

Зі зростанням функціоналу, прив'язаного до Інтернету речей (IoT), значна частина важливих для розслідування даних, включаючи геолокацію, історію поїздок та функції дистанційного керування, зберігається на віддалених серверах виробників транспортних засобів. Вилучення цих даних із зовнішніх динамічних джерел здійснюється методом API-орієнтованого отримання. Цей метод є наріжним каменем сучасної криміналістики, оскільки хмарне сховище часто містить сліди, які не можуть бути змінені зловмисником безпосередньо в авто-

мобілі. Проте успішність і, головне, форензична надійність цього процесу прямо залежить від його прозорості. Для забезпечення цілісності та автентичності отриманих хмарних даних необхідно впроваджувати розширене логування усіх комунікаційних параметрів, включаючи заголовки та методи HTTP (HyperText Transfer Protocol (*протокол передавання гіпертексту*) – примітка Д. Ч.), що забезпечує відстежуваність доказу. Обов'язковою умовою вилучення таких даних у кримінальному провадженні є збереження та подальше порівняння контрольної суми (хешу) первинно отриманих файлів та їх подальших копій[1].

Висновки. На основі проведеного аналізу встановлено, що незаконне заволодіння транспортними засобами трансформувалося у високотехнологічну злочинну діяльність, що систематично включає використання спеціальних засобів (як-от кодграбери-ретранслятори) і вимагає, у тому числі, кваліфікації за ч. 2 ст. 361 КК України (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж). У зв'язку з цим цифрова криміналістика повинна більш глибоко вивчати методи, що охоплюють множинні джерела слідів: вбудовані системи, хмарні сервери та побічні канали мобільних пристроїв.

Ключовим викликом для забезпечення доказової цінності залишається відсутність захищеного від втручання сховища даних у транспортних засобах, що підвищує ризики маніпуляцій і вимагає обов'язкового застосування протоколів розширеного логування для гарантування форензичної надійності та відтворюваності доказів.

Проведений аналіз сучасних способів незаконного заволодіння транспортними засобами дозволив сформулювати такі рекомендації для боротьби з аналізованими правопорушеннями:

1. Для науковців у галузі криміналістики:

– продовжити наукові пошуки з метою пошуку шляхів захисту від несанкціонованого втручання у сховища даних транспортних засобів;

– розробити методи, які дозволять чітко артикулювати ступінь імовірності та можливі джерела помилок результатів технічних розслідувань;

– дослідити шляхи впровадження динамічної системи сертифікації кібербезпеки для автоматизованих транспортних засобів та аналіз ризиків, зокрема, пов'язаних із крадіжкою інтелектуальної власності.

2. Для практичних співробітників правоохоронних органів:

– завжди розглядати використання злочинцями спеціальних технічних засобів (кодграберів-ретрансляторів) як ознаку несанкціонованого втручання в роботу електронно-обчислювальних систем (ч. 2 ст. 361 КК України);

– при розслідуванні незаконного заволодіння транспортними засобами приділяти першочергову увагу мобільним пристроям підозрюваних, оскільки вони є своєрідними «шлюзами» для доступу до хмарних даних;

– під час проведення API-орієнтованого отримання даних застосовувати протоколи, що вимагають розширеного логування всіх комунікаційних параметрів для забезпечення відстежуваності та надійності доказів.

3. Для судових експертів (у тому числі судових експертів-криміналістів):

– забезпечувати гарантовану відтворюваність та прозорість експертного дослідження та його результатів;

– детально фіксувати (документувати) інформацію про походження даних, виявлених під час експертних досліджень слідів незаконного заволодіння транспортними засобами.

[1] Ebbers S. 'Grand theft API: A forensic analysis of vehicle cloud data' *Forensic Science International: Digital Investigation* (2024) DOI: https://doi.org/10.1016/j.fsidi.2023.301691

REFERNSES

Legal documents

Cases

1. Postanova Verkhovnoho Sudu vid 24 veresnia 2019 roku u kryminalnomu provadzhenni № 12016100040004640 (sprava № 755/13969/16-k) URL: https://reyestr.court.gov.ua/Review/75970298 (in Ukranian)
2. Postanova Verkhovnoho Sudu vid 02 zhovtnia 2025 roku u kryminalnomu provadzhenni № 12019160490003587 (sprava № 523/503/20) [URL: https://reyestr.court.gov.ua/Review/130683584 (in Ukranian)

3. Stratehiia pidvyshchennia rivnia bezpeky dorozhnoho rukhu v Ukraini na period do 2024 roku. Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 21 zhovtnia 2020 r. № 1360-r. URL: https://zakon.rada.gov.ua/laws/show/1360–2020-%D1%80#Text (in Ukranian)
4. Ukhvala Apeliatsiinoho sudu m. Kyieva vid 08 serpnia 2018 roku u kryminalnomu provadzhenni № 12016100040004640 (sprava № 11-kp/796/995/2018) URL: https://reyestr.court.gov.ua/Review/75970298 (in Ukranian)
5. Ukhvala Kyivskoho apeliatsiinoho sudu vid 19 serpnia 2020 roku u kryminalnomu provadzhenni pid № 12017100040007894 (sprava № 754/13878/17) URL: https://reyestr.court.gov.ua/Review/91185733 (in Ukranian)
6. Ukhvala Poltavskoho apeliatsiinoho sudu vid 13 veresnia 2022 roku u kryminalnomu provadzhenni № 12016220060000877 (sprava № 646/110/17 URL: https://reyestr.court.gov.ua/Review/106413158 (in Ukranian)
7. Ukhvala Kyivskoho apeliatsiinoho sudu vid 12 lystopada 2024 roku u kryminalnomu provadzhenni № 11-kp/824/3216/2024 (sprava № 754/5026/20) URL: https://reyestr.court.gov.ua/Review/123038410 (in Ukranian)
8. Rezoliutsiia Heneralnoi Asamblei OON vid 31 serpnia 2020 roku Pidvyshchennia bezpeky dorozhnoho rukhu v usomu sviti URL: https://docs.un.org/en/a/res/74/299 (in Ukranian)

Bibliography

Authored books

1. Holina V. V., Shramko S. S. *Kulturolohiia bezpeky dorozhnoho rukhu v Ukraini: teoriia ta praktyka zapobihannia avtotransportnym pravoporushenniam: monohrafiia* [Culturology of road safety in Ukraine: theory and practice of preventing motor vehicle offenses: monograph] (Pravo, 2023) 184. <DOI:10.31359/9789669986870> (in Ukranian)
2. Kolodiazhnyi M. H. *Stratehiia Vision Zero: uroky dlia Ukrainy: monohrafiia* [Vision Zero Strategy: Lessons for Ukraine: Monograph] (Pravo, 2022) 300. <URL: https://ivpz.kh.ua/wp-content/uploads/2022/11/%D0%9A%D0%BE%D0%BB%D0%BE%D0%B4%D1%8F%D0%B6%D0%BD%D0%B8%D0%B9.-%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F-Vizion-zero_. pdf> (in Ukranian)
3. Ludger Hovestadt, Vera Bühlmann, *A Quantum City: Mastering the Generic* (Birkhäuser, 2015) 824. < https://dokumen.pub/a-quantum-city-mastering-the-generic-1nbsped-9783035606416–9783035606263.html>

Non-authored books

4. *Vision zero toolkit* (Department of Transportation in the interest of information exchange, 2024) 55. <https://highways.dot.gov/sites/fhwa.dot.gov/files/2024–04/Vision%20Zero%20Toolkit%20508_0.pdf>

Jornal articles

5. Batyrhareieva V. S. 'Naukovo-tekhnichnyi prohres i pravoporushennia u sferi bezpeky dorozhnoho rukhu ta ekspluatatsii transportu: okremi rakursy problemy' [Scientific and technical progress and offenses in the field of road traffic safety and transport operation: separate perspectives of the problem] (2024) 48 Pytannia borotby zi zlochynnistiu 103. DO I: 10.31359/2079-6242-2024-48-103 (in Ukranian)
6. Holina V. V. 'Zapobihannia transportnym pravoporushenniam v Ukraini v konteksti yevrointehratsii' [Prevention of transport offenses in Ukraine in the context of European integration] (2022) 4 Naukovyi zhurnal Pivdenno-ukrainskyi pravnychyi chasopys 61. DOI: https://doi.org/10.31359/9789669986870 (in Ukranian)
7. Holina V. V. 'Vplyv zarubizhnykh praktyk zabezpechennia bezpeky dorozhnoho rukhu na kontseptsii zapobihannia transportnym pravoporushenniam v Ukraini' [The influence of foreign road safety practices on the concepts of preventing transport offenses in Ukraine] (2024) 47 Pytannia borotby zi zlochynnistiu 124. DOI: 10.31359/2079-6242-2024-47-124 (in Ukranian)
8. Ebbers S, Gens S, Bakkouch M, Freiling F, Schinzel S. 'Grand theft API: A forensic analysis of vehicle cloud data' (2024) 48 Forensic Sci Int: Digit Invest 301691. DOI:10.1016/j.fsidi.2023.301691
9. Meteňko J, Meteňková M. 'Digital trace as a personal and criminalistics object' (2024) 9(1) Security Horizons 175. DOI: 10.35603/sws.iscss.2024/s02/12
10. Wessing R. Akteneinsichtsrecht, Besichtigungsrecht; Auskunftsrecht des Beschuldigten (Beck'scher Onlinekommentar StPO mit RiStBV und MiStra, 2018). DOI: 10.1515/9783110630244–020
11. Yang Q, Gasti P, Zhou G, Farajidavar A, Balagani K. 'On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel' (2017) IEEE T Inf Forens Sec. DOI:10.1109/TIFS.2016.2639446

Conference paper

12. Batyrhareieva V. S. 'Okremi fokusy problemy avtotransportnoi bezpeky v Ukraini' [Separate foci of the problem of road safety in Ukraine] *Derzhavna polityka u sferi ubezpechennia dorozhnoho rukhu: teoriia, zakonodavstvo, praktyka* (Pravo, 2021) DOI: 10.31359/978-966-998-313-8 (in Ukranian)

Чекін Д. О.

Методи і засоби цифрової криміналістики у боротьбі з незаконним заволодінням транспортними засобами

У статті представлено комплексне дослідження, присвячене виокремленню типових способів незаконного заволодіння транспортними засобами шляхом використання цифрових технологій та застосуванню спеціалізованих методів і засобів цифрової криміналістики в контексті боротьби з високотехнологічним незаконним заволодінням транспортними засобами. Актуальність теми дослідження та постановка проблеми обґрунтовані тим, що стрімкий науково-технічний прогрес у поєднанні із всеохоплюючою цифровізацією автомобільного сектору докорінно змінили ландшафт злочинної діяльності. Сучасні майнові злочини все частіше включають несанкціоноване втручання в роботу електронних систем та бортового обладнання за допомогою складних технічних комплексів, таких як кодграбери та ретранслятори сигналу. Ця технологічна трансформація зумовлює необхідність зміни парадигми у сфері цифрової криміналістики, вимагаючи негайної адаптації для забезпечення збереження, вилучення та доказової цінності цифрових слідів, отриманих із цих нових та вкрай нестабільних джерел.

Основною метою цього дослідження є виявлення, систематизація та визначення типових способів незаконного заволодіння транспортними засобами та методів цифрової криміналістики, застосовних до боротьби із сучасними злочинами аналізованої категорії, а також формулювання дієвих практичних рекомендацій для відповідних суб'єктів. Методологічна основа дослідження дозволила провести аналіз існуючих вразливостей у системі безпеки автомобілів. У ході дослідження встановлено, що критичним викликом для цієї сфери є притаманна недосконаліть механізмів захисту від втручання у джерела для зберігання даних про транспортні засоби, що створює значний ризик маніпулювання даними або їх втрати через дії зловмисників. Крім того, у дослідженні наголошується, що для гарантування цілісності та судової допустимості отриманих даних необхідним є впровадження протоколів розширеного логування під час процесу вилучення даних.

Сформульовано набір цільових практичних рекомендацій для підвищення ефективності розслідувань. Для наукової спільноти акцент зроблено на необхідності подальшого дослідження інноваційних рішень, що забезпечують повну відтворюваність проведених криміналістичних досліджень. Правоохоронним органам рекомендовано надати пріоритет належному технічному забезпеченню спеціальними мобільними криміналістичними пристроями та суворому дотриманню процедур логування для збереження ланцюга доказів. Для судових експертів у статті підкреслюється необхідність прозорого представлення результатів із чітким визначенням ймовірності висновків та ідентифікацією потенційних джерел помилок з метою відповідності суворим стандартам системи правосуддя.

Ключові слова: *цифрова криміналістика, незаконне заволодіння транспортними засобами, кодграбер, хмарні дані, API-орієнтоване отримання, доказова цінність.*

Chekin D. O.

Methods and Tools of Digital Forensics in Combating Vehicle Theft

The article presents a comprehensive study dedicated to identifying typical methods of illegal vehicle seizure through the utilization of digital technologies and the application of specialized digital forensics methods and tools in the context of combating high-tech vehicle theft. The relevance of the research topic and the problem statement are substantiated by the fact that rapid scientific and technical progress, combined with the pervasive digitalization of the automotive sector, have fundamentally altered the landscape of criminal activity. Modern property crimes increasingly involve unauthorized interference with the operation of electronic systems and on-board equipment using complex technical complexes, such as code grabbers and signal relay devices. This technological transformation necessitates a paradigm shift in the field of digital forensics, requiring immediate adaptation to ensure the preservation, extraction, and evidentiary value of digital traces obtained from these new and highly volatile sources.

The primary objective of this study is the identification, systematization, and definition of typical methods of illegal vehicle seizure and digital forensics methods applicable to combating modern crimes of this category, as well as the formulation of effective practical recommendations for relevant entities. The methodological basis of the study facilitated an analysis of existing vulnerabilities in vehicle security systems. The study established that a critical challenge for this sphere is the inherent imperfection of protection mechanisms against interference with vehicle data storage sources, which creates a significant risk of data manipulation or loss due to malicious actions. Furthermore, the study emphasizes that implementing extended logging protocols during the data extraction process is necessary to guarantee the integrity and judicial admissibility of the obtained data.

A set of targeted practical recommendations has been formulated to enhance the effectiveness of investigations. For the scientific community, emphasis is placed on the need for further research into innovative solutions that ensure the full reproducibility of forensic examinations conducted.

Law enforcement agencies are recommended to prioritize proper technical support with special mobile forensic devices and strict adherence to logging procedures to preserve the chain of evidence. For forensic experts, the article highlights the necessity of transparent presentation of results with a clear definition of the probability of conclusions and the identification of potential sources of error to comply with the rigorous standards of the justice system.

Keywords: *digital forensics, illegal vehicle theft, code grabber, cloud-data, API-based acquisition, evidentiary value.*

Стаття надійшла до редакції:27.10. 2025 р.
Прийнята до друку: 20.11.2025 р.