

Перелік джерел посилання

1. Winburn A. P., Tallman S. D. Forensic Anthropology. Encyclopedia of Forensic Sciences, Third Edition (Third Edition). 2023. No 2. Pp. 482—492. DOI: 10.1016/ B978-0-12-823677-2.00082-9 (дата звернення: 31.08.2023).
2. Helm K., Matzenauer C., Neuhuber F., Monticelli F., Meyer H., Pittner S., Gotsmy W. Suitability of specific soft tissue swabs for the forensic identification of highly decomposed bodies. *International journal of legal medicine*. 2021. No 135(4). Pp. 1319—1327. DOI: 10.1007/s00414-021-02601-3 (дата звернення: 31.08.2023).
3. Костіков І. Ю., Марійко В., Щербакова Ю. В., Мартиненко С. В., Сіривля А. І., Сандалович Б. О., Аббасов Р. Г. Молекулярно-генетична ідентифікація осіб, загиблих під час російської збройної агресії проти України: успіхи та проблеми. *Криміналістичний вісник*. 2023. Вип. 39(1). С. 10—28. DOI: 10.37025/ 1992-4437/2023-39-1-10 (дата звернення: 31.08.2023).
4. Latham K. E., Miller J. J. DNA recovery and analysis from skeletal material in modern forensic contexts. *Forensic sciences research*. 2018. No 4(1). Pp. 51—59. DOI: 10.1080/20961790.2018.1515594 (дата звернення: 31.08.2023).
5. Emery M. V., Bolhofner K., Ghafoor S., Winingear S., Buikstra J. E., Fulginiti L. C., Stone, A. C. Whole mitochondrial genomes assembled from thermally altered forensic bones and teeth. *Forensic science international. Genetics*. 2022. No 56. Pp. 102610. DOI: 10.1016/j.fsigen.2021.102610 (дата звернення: 31.08.2023).
6. Про державну реєстрацію геномної інформації людини : Закон України від 09.07.2022 р. No 2391-IX. URL: <https://zakon.rada.gov.ua/laws/show/2391-20#Text> (дата звернення: 31.08.2023).

**Використання програми Cybid V-SIM 4.0 під час проведення
автотехнічної експертизи**

Юрій Бодоряк,

Тернопільський НДЕКЦ МВС України, м. Тернопіль, Україна, e-mail: expert.yd@gmail.com

Юрій Шминдюк,

Тернопільський НДЕКЦ МВС України, м. Тернопіль, Україна, e-mail: shmyndyuk.yurii@gmail.com

Юрій Пипко,

Тернопільський НДЕКЦ МВС України, м. Тернопіль, Україна, e-mail: ternopol@ndekc.mvs.gov.ua

Використання комп'ютерної програми Cybid V-SIM під час проведення автотехнічних експертиз забезпечує глибокий і точний аналіз обставин дорожньо-транспортних пригод, оцінює вплив окремих факторів на її розвиток та дає можливість аналізувати процеси і наслідки зіткнення транспортних засобів між собою, з іншими учасниками руху або з навколишніми перешкодами.

Ключові слова: дорожньо-транспортна пригода; автотехнічна експертиза; CYBID V-SIM 4.0; механізм зіткнення; моделювання руху.

**Use of Cybid V-SIM 4.0 Software as a Practical Tool During
Automotive Technical Examination**

Yurii Bodoriak, Yurii Shmyndiuk, Yurii Pypko

The practical application of the Cybid V-SIM software during automotive technical examinations facilitates a deeper and more accurate analysis of circumstances surrounding road traffic accidents. It allows for evaluating the impact of individual factors on their development and enables the analysis of the processes and consequences of vehicle collisions with each other, other traffic participants, or surrounding obstacles.

Keywords: Road Traffic Accident; Automotive Technical Examination; Collision Mechanism; Motion Modeling.

Програма *Cybid V-SIM* дає можливість моделювати рухи транспортних засобів — автомобілів, причепів і напівпричепів у різноманітному дорожньому середовищі, із урахуванням законів динаміки руху як поодиноких, так і складних транспортних засобів у тривимірному режимі [1, с. 11].

Обстановка дорожньо-транспортної пригоди (далі — ДТП) містить комплекс даних, що характеризуються умовами, за яких вона виникла, тривала та завершилася.

Механізм зіткнення транспортних засобів — це комплекс пов'язаних об'єктивними закономірностями обставин, що визначають процес зближення транспортних засобів перед зіткненням, їх взаємодію під час удару та подальший рух до зупинки [4, с. 195].

Із метою попереднього аналізу механізму зіткнення транспортних засобів за допомогою програмного комплексу *Cybid V-SIM* було проведено моделювання їх руху, для чого на стадії їх взаємного зближення було використано певні значення технічних величин (швидкості руху, завантаження та розташування відносно елементів дороги). Моделювання взаємодії транспортних засобів у момент їх первинного контактування (див. рис. 1 та 2) проводили з урахуванням результатів відповідної транспортно-трасологічної експертизи.



Рис. 1. Взаємодія транспортних засобів в момент первинного контактування

Моделювання руху транспортних засобів на стадії їх відкидання відбувалось автоматично за алгоритмами роботи програмного комплексу *Cybid V-SIM*. Під час моделювання (реконструкції) було визначено, що після контактної взаємодії транспортні засоби переміщувалися до місць їх зупинки, проте їх змодельоване кінцеве розташування відносно елементів дороги не відповідало фактичному (зафіксованому у відповідному протоколі огляду місця події, рис. 3).

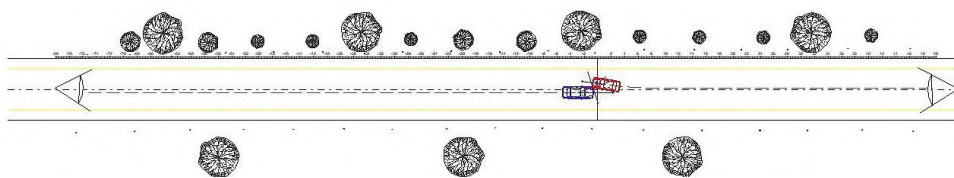


Рис. 2. Моделювання механізму зіткнення відносно результатів транспортно-трасологічної експертизи

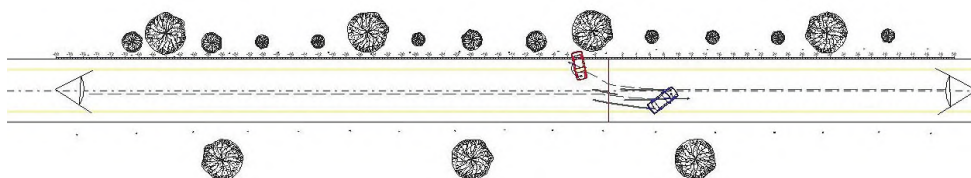


Рис. 3. Запропоноване моделювання відкидання та кінцевого розташування транспортних засобів програмою *Cybid V-SIM*

Надалі було проведено численні спроби коригування результатів реконструкції шляхом зміни (підбирання) значень технічних величин у межах заданих діапазонів та похибок, проте в результаті жодної зі спроб не вдалося отримати результат, за якого змодельоване кінцеве розташування транспортних засобів відповідало б фактичному. На перший погляд, подібні результати могли б стати передумовою для висунення гіпотези про технічну неспроможність вихідних даних, проте вони не дають достатніх підстав для такого обґрунтованого висновку, оскільки цей програмний комплекс є доволі точним інструментом, а його алгоритми вимагають введення точних абсолютних значень величин. На противагу цьому, отримані дані під час проведення слідчого експерименту базуються на показаннях, тобто на суб'єктивному сприйнятті реальності й можуть не відповідати з достатньою точністю фактичним (об'єктивним) даним. Водночас достатніми підставами констатувати технічну неспроможність вихідних даних могли б бути результати, за яких траєкторії руху транспортних засобів у процесі їх переміщення на стадії відкидання суттєво відрізнялися б від фактичних напрямків переміщення (наприклад, були б діаметрально протилежними до фактичних).

Під час проведення досліджень такого варіанту розвитку ДТП поміж інших було висунуто гіпотезу щодо технічної можливості водіям транспортних засобів уникнути ДТП шляхом виконання ними вимоги «дати дорогу» в частині «звільнити займану смугу руху». Для цього було проведено відповідні розрахунки та визначено, що із заданого моменту настання взаємної конкретної видимості з робочих місць водіїв транспортних засобів вони мали технічну можливість виконати маневр «зміна смуги руху» для повернення на свою смугу руху з урахуванням необхідного поперечного зміщення та безпечного бокового інтервалу (рис. 4).



Рис. 4. Вигляд з місця водія під час маневру роз'їзду для уникнення ДТП

Висунута гіпотеза також знайшла своє підтвердження за умови своєчасного виконання водіями зазначених маневрів із заданого моменту настання взаємної конкретної видимості зі своїх робочих місць і збереження ними подальшої прямолінійної траєкторії у межах своїх смуг для руху, тому зіткнення транспортних засобів із технічної точки зору виключалося. Із метою наочної візуальної демонстрації результатів проведеного дослідження за допомогою програмного комплексу *Cybid V-SIM* було проведено моделювання руху транспортних засобів із застосуванням значень величин, отриманих за допомогою попередніх розрахунків.

Слід зазначити, що використання програмного комплексу *Cybid V-SIM* як інструменту для реконструкції механізму розвитку ДТП із метою перевірки технічної спроможності вихідних даних можливе, проте з певними застереженнями та обмеженнями. Тому видається перспективним застосування цього програмного комплексу з використанням величин технічних даних, отриманих шляхом проведення експертиз фото- та відеозаписів або із записів автомобільних реєстраторів даних про події (*EDR*), оскільки такі дані є найбільш об'єктивними та дають змогу проводити реконструкції з максимальною достовірністю.

Цей програмний комплекс — якісний інструмент для моделювання руху транспортних засобів із метою візуальної наочної демонстрації певних етапів у розгортанні події або демонструванні результатів автотехнічної експертизи. До того ж корисним є його функціонал, що дає змогу використовувати під час моделювання супутникові знімки місцевості для відображення реальних дорожніх умов.

Перелік джерел посилання

1. CYBID V-SIM 4.0. Моделирование движения и столкновений автотранспортных средств. Руководство пользователя. Краков, 2018. Версия документа 1.0 (версия программы 4.0). Лицензия № 67D6D200.
2. Дубінін О. А. Використання ПЕОМ при моделюванні механізму ДТП : методичні рекомендації. Київ, 2007. 49 с.
3. Кристи Н. М. Методические рекомендации по производству автотехнической экспертизы. Москва, 1971. 112 с.
4. Судебная автотехническая экспертиза. Часть II. Теоретические основы и методики экспертного исследования при производстве автотехнической экспертизы : пособие для экспертов автотехников, следователей и судей / отв. ред. В. А. Иларионова. Москва, 1980. 392 с.

Журнали подій операційних систем *Windows* у комп'ютерно-технічній експертизі

Юрій Божко,

Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: yuriybozhko93job@gmail.com

Досліджено журнали операційних систем сімейства Windows, наведено перелік типових журналів, які в ній існують, проаналізовано записи цих журналів, оцінено роль таких журналів у цифровій криміналістиці.

Ключові слова: журнали подій; операційні системи; Windows; цифрова криміналістика; Event Logs; журнал безпеки; журнал системи; журнал додатків.

Event Logs of Windows Operating Systems in Computer Technical Expertise

Yurii Bozhko

Logs of operating systems of the Windows family were studied; a list of typical logs that existing in is given; the records of these logs were analyzed; role of such logs in digital forensics is assessed.

Keywords: event logs; operating systems; Windows; digital forensics; Event logs; security log; system log; application log.

Цифрова криміналістика в сучасному світі технологій відіграє важливу роль у розкритті, розслідуванні та протидії злочинам, які відбуваються з використанням комп'ютерної техніки. Через популярність конкретних операційних систем вони можуть стати мішенню для зловмисників. Одними з найпопулярніших сьогодні є операційні системи сімейства *Windows*. Значну роль у розслідуванні кіберінцидентів і злочинів, у яких фігурує комп'ютерна техніка, відіграють журнали подій операційних систем, які в певному вигляді існують майже в кожній операційній системі.

У цифровій криміналістиці журнали подій можна використовувати для виявлення зловмисницької діяльності: аналіз журналів подій сприяє виявленню незвичної та підозрілої активності (наприклад, несподіваних входів, невдалих спроб доступу, зміни конфігурації системи тощо). Такі події можуть свідчити про можливі спроби несанкціонованого доступу або активність шкідливого програмного забезпечення. Також аналіз журналів подій допомагає встановити послідовність подій, що призвели до інциденту, і дає змогу відновити хронологію дій зловмисників. Журнали подій, зокрема, можна використати як докази в судових справах: для підтвердження або