УДК 341.4:004.9
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/55

Семенов С. В.
https://orcid.org/0009-0004-1882-1488
Кам'янець-Подільський національний університет імені Івана Огієнка

Адамовський В. І.
https://orcid.org/0000-0002-9186-6234
Кам'янець-Подільський національний університет імені Івана Огієнка

СТАНДАРТИ ЦИФРОВОГО ДОКАЗУВАННЯ У МІЖНАРОДНОМУ КРИМІНАЛЬНОМУ ПРАВІ: ЧОТИРИРІВНЕВА МОДЕЛЬ ДЛЯ СПРАВ ПРО ДЕПОРТАЦІЮ ТА ПРИМУСОВЕ ПЕРЕМІЩЕННЯ УКРАЇНСЬКИХ ЦИВІЛЬНИХ

Статтю присвячено стандартам збирання, збереження, перевірки, подання та оцінювання цифрових доказів у міжнародному кримінальному праві й їх адаптації до проваджень щодо депортації та примусового переміщення українських цивільних. На основі структурованого доктринального і порівняльного контент-аналізу Римського статуту, Правил процедури та доказування Міжнародного кримінального суду, Елементів злочинів, релевантної практики МКС, інструментів «м'якого права» та матеріалів міжнародних механізмів щодо України визначено межі технологічно нейтральної моделі вільної оцінки доказів. Уточнено співвідношення понять «цифровий доказ», «цифрово похідний доказ», «цифрова інформація з відкритих джерел» і «доказ, створений користувачем». Показано, що технічна цілісність файла не доводить правдивості його змісту, а встановлення акаунта, номера або пристрою не є автоматичним встановленням автора чи суб'єкта злочину. Запропоновано чотирирівневу модель перевірки: 1) походження і цілісність; 2) змістова верифікація; 3) атрибуція; 4) юридико-контекстуальна достатність. Новизна моделі полягає не у створенні універсального технічного стандарту, а в поєднанні наявних процедур перевірки з окремими юридичними тестами для воєнного злочину депортації або переміщення, злочину проти людяності у формі депортації чи насильницького переміщення та насильницької передачі дітей як діяння, передбаченого статтею 6(e) Римського статуту. Модель апробовано на матеріалах справ Al-Werfalli, Al Hassan, Yekatom and Ngaïssona та українського доказового масиву 2023–2026 років. Обґрунтовано, що доказова сила виникає зі збіжності перевірених і, за можливості, незалежних цифрових та документальних матеріалів, показань і експертних висновків; жоден «мінімальний пакет» не гарантує допустимості або достатності поза контекстом конкретного обвинувачення.

Ключові слова: *цифрові докази, цифрова інформація з відкритих джерел, OSINT, міжнародне кримінальне право, депортація, примусове переміщення, Міжнародний кримінальний суд, автентифікація, атрибуція, права дитини.*

Постановка проблеми. Цифровізація збройних конфліктів змінила архітектуру доказування міжнародних злочинів. Фото і відео зі смартфонів, дописи посадових осіб, супутникові зображення, електронні реєстри, телекомунікаційні дані та листування можуть фіксувати окремі ланки депортації або примусового переміщення: створення примусового середовища, реєстрацію, транспортування, розміщення, зміну документів, передачу дітей чи перешкоджання поверненню. Однак доступність такого матеріалу не усуває питань про походження, незмінність, контекст, автора та зв'язок із конкретним елементом злочину.

Римський статут не встановлює окремого режиму для цифрових доказів. Стаття 69(4) вимагає оцінювати належність, доказову цінність і можливу шкоду справедливому розгляду або справедливій оцінці показань; правила 63(2)

© Семенов С. В., Адамовський В. І., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

і 63(4) закріплюють свободу оцінювання та відсутність загальної юридичної вимоги corroboration [1, ст. 69(4); 2, правила 63(2), 63(4)]. Тому технічна автентифікація не є «сертифікатом допустимості»: суд має бачити прозорий перехід від цифрового об'єкта до фактичного, а потім юридичного висновку.

Аналіз останніх досліджень і публікацій. Сучасна література окреслює чотири групи ризиків. Дослідження відкритих джерел виявляють платформну, алгоритмічну, мовну та когнітивну селекцію [11, с. 89–102]; праці про експертні докази й права захисту наголошують на відтворюваності методу, доступі до даних та можливості перевірити висновок [12, с. 674–686; 13, с. 756–765]. Аналіз UGE, deepfakes і криптографічного засвідчення показує, що хеш підтверджує незмінність після контрольного моменту, але не правдивість первинного змісту [14, с. 5–28; 15, с. 251–254; 16, с. 861–868].

Емпіричне опитування суддів МКС фіксує занепокоєння обсягом UGE, дезінформацією, джерельною упередженістю та підготовленістю юристів [17, с. 3, 10–19, 23], а кількісний аналіз практики Суду демонструє нерівномірність реального використання цифрових матеріалів [18, с. 112–124]. Праці K. Gavrysh та H. Kuczyńska розвивають українську і візуально-наративну перспективи [19, с. 114–126; 20]. Натомість зв'язок між технічними стадіями перевірки та відмінними елементами депортації, примусового переміщення і передачі дітей залишається недостатньо систематизованим.

Постановка завдання. Мета статті – уточнити сучасні стандарти цифрового доказування в міжнародному кримінальному праві та запропонувати модель, яка локалізує доказовий розрив між цифровим об'єктом і конкретним елементом злочину. Дослідження виконано як структурований доктринальний і порівняльний контент-аналіз, а не як систематичний огляд.

Корпус охопив Римський статут, Правила процедури та доказування, Елементи злочинів, норми міжнародного гуманітарного права, оприлюднену практику МКС, інструменти «м'якого права», рецензовані праці та матеріали міжнародних механізмів щодо України. Пошук здійснювався українською й англійською мовами в базах МКС, HUDOC, ООН, УВКПЛ, МКЧХ, ОБСЄ, на сайтах видавців та в академічних репозитаріях. Включалися джерела, що визначають процедуру роботи з цифровим матеріалом, стандарт його оцінювання або фактичну модель переміщення; виключалися дублікати, неперевірені агрегатори та матеріали без простежуваного походження.

Одиницею аналізу було твердження про: 1) походження чи незмінність; 2) місце, час або зміст; 3) автора, користувача чи організаційний зв'язок; 4) елемент злочину або форму відповідальності. Для кожного твердження зіставлялися контрольне питання, тип джерела, альтернативне пояснення й наслідок помилки. Модель апробовано на практиці МКС і на українському масиві 2023–2026 років. Обмеження зумовлені відсутністю доступу до закритих матеріалів, первинних пристроїв і серверних даних платформ; тому висновки стосуються методики перевірки, а не вини конкретних осіб.

Виклад основного матеріалу дослідження. Понятійні та нормативні межі. «Цифровий доказ» у цій статті означає інформацію, створену, записану, передану або збережену в цифровій формі та запропоновану для встановлення факту. Digitally derived evidence є результатом відбору, оброблення чи візуалізації первинних даних; digital open source information (DOSI) – інформацією з публічних вебресурсів, яка набуває доказового значення після документованого збирання й перевірки [6, с. 3–4; 7, с. 3–4]. User-generated evidence (UGE) створює звичайна особа на персональному пристрої; воно може бути публічним або непублічним [14, с. 5–28; 17, с. 5–8]. Ці категорії перетинаються, але не є взаємозамінними.

Нормативна архітектура має різні функції. Статут і Правила задають процесуальну рамку, а Елементи злочинів і міжнародне гуманітарне право – предмет доказування [1–5]. Апеляційна практика МКС розмежовує прийняття матеріалу й остаточну оцінку його ваги [21]. Берклійський протокол, Лейденські настанови, спільний посібник Eurojust/OTP та керівництво для суддів деталізують планування, збирання, збереження, верифікацію, етичні гарантії й представлення [6, с. 16–93; 7, с. 10–53; 8, с. 5–14, 43–49; 9, с. 10–30]. Протокол E-Court у провадженні Duterte є корисним прикладом технічної організації доказів, але не універсальним джерелом права МКС [10].

Практика МКС і матеріали щодо України. Ордер Al-Werfalli істотно спирався на публічно поширені відео, але не сформулював універсального тесту для соціальних мереж [22, пп. 11–22]. У справі Al Hassan аудіовізуальні матеріали оцінювалися в ширшій доказовій сукупності [23]. Вирок у справі Yekatom and Ngaïssona аналізує Facebook-матеріали, call detail records та електронні листи й показує різну силу висновків про

контроль акаунта, автора повідомлення та організаційний зв'язок; вирок оскаржено, тому він не є остаточним [24; 25]. Практика підтверджує гнучке оцінювання, але не дозволяє ототожнювати метадані, контроль пристрою й кримінальну відповідальність.

У ситуації в Україні публічний матеріал МКС щодо ордерів від 17 березня 2023 року визначає кваліфікацію, але не розкриває повної доказової основи [26]. Звіт Московського механізму ОБСЄ систематизує маршрути, документи, зміни статусу й перешкоди поверненню дітей [27, с. 12–26, 40–45, 53–56]. Велика палата ЄСПЛ встановила порушення, пов'язані з переміщенням, передачею та усиновленням українських дітей, однак її предмет і стандарт доказування не тотожні кримінальному провадженню [28, пп. 1594–1599].

Комісія ООН верифікувала групу щонайменше 1205 дітей, спираючись на інтерв'ю, документи, виїзні відвідування та відкриті джерела [29, пп. 7–10, 64–65]. УВКПЛ описало примусове переміщення дорослих і дітей через адміністративний тиск, затримання, погрози та перешкоди поверненню [30, пп. 28–49, 57–64]. Yale HRL і Starling Lab демонструють можливості супутникового аналізу, відкритих реєстрів і криптографічного засвідчення, але є описами власних дослідницьких або технічних проєктів, а не судовою валідацією [31; 32]. Отже, цифрові сліди мають зіставлятися з документами, показаннями та експертними висновками.

Чотирирівнева модель перевірки. Модель організовує перевірку за силою висновку, а не видом носія. Один об'єкт може бути технічно цілісним, але слабким для атрибуції чи юридичної кваліфікації. Рівні не є формальними стадіями допустимості: це карта доказових розривів, яка вимагає для кожного твердження зафіксувати джерело, метод, результат, невизначеність, альтернативне пояснення та матеріал, потрібний для його перевірки (табл. 1).

Наскрізною вимогою є незалежність підтверджень: два дописи можуть походити з одного ролика, а кілька новин – з однієї заяви. Слабкість окремого рівня іноді компенсується іншими матеріалами, але не припущенням. Результат перевірки може бути позитивним, негативним або обмежувальним: наприклад, повідомлення без установленого автора може зберігати контекстуальну, але не індивідуалізуючу вагу.

Окремі юридичні тести. Четвертий рівень застосовується лише після формулювання конкретної кваліфікації. Воєнний злочин, злочин проти людяності та насильницька передача дітей за статтею 6(e) мають різний предмет доказування; однаковий факт руху людей не дає однакового юридичного висновку (табл. 2).

Для воєнного злочину потрібно перевіряти захищений статус осіб, територіальний напрям, окупацію та фактичні умови заявленої евакуації. Для статті 7(1)(d) примус може випливати з погроз, затримання, психологічного тиску чи зловживання владою, але окремо доводяться контекст нападу й знання. Для статті 6(e) дані про зміну імен, громадянства, опіки, виховання та перешкоди поверненню можуть підтримувати аналіз передачі й наміру, проте спеціальний намір не можна презюмувати. В усіх моделях посада пояснює доступ до ресурсів, але не встановлює автоматично наказ, внесок або контроль.

Апробація та процесуальні гарантії. У сценарії цифрової комунікації Yekatom and Ngaïssona перший рівень охоплює джерело, повноту гілки й незмінність; другий – зміст, переклад і часову послідовність; третій – зв'язок акаунта з користувачем через платформні дані, CDR та інші контакти; четвертий – значення повідомлення для конкретного діяння й форми відповідальності [24]. У сценарії реєстру українських дітей ті самі рівні вимагають історії експорту, дедуплікації, перевірки маршрутів, встановлення контролю над полями та зіставлення запису з правовим статусом і способом передачі. Кількісні висновки мають містити дату зрізу, правила підрахунку й діапазон невизначеності.

Ключові гарантії – відтворюване розкриття, збереження master-файла й контрольованих копій, журнал операцій, версії програмного забезпечення, часові зони та документовані перетворення [6–9; 16]. Автоматичне розпізнавання, переклад чи генеративні моделі створюють похідний об'єкт: їх результат потребує валідації, опису помилок і людської перевірки; універсального надійного детектора синтетичного контенту немає [15; 17]. Для даних дітей діють мінімізація, розмежування відкритої та захищеної версій, контроль доступу й оцінка ризику повторної ідентифікації [8, с. 11–14, 43–49; 29, пп. 7–13].

Висновки:

1. Технологічно нейтральна модель МКС не створює окремого тесту допустимості для цифрових доказів. Походження, цілісність, зміст, атрибуція і юридичне значення є пов'язаними, але самостійними питаннями.

2. Запропонована чотирирівнева модель поєднує наявні технічні процедури з картою еле-

Таблиця 1

Чотирирівнева модель перевірки цифрових доказів

Рівень	Контрольне питання	Орієнтовні матеріали	Типова помилка
1. Походження і цілісність	Звідки походить об'єкт і що з ним відбувалося?	Найраніша версія; URL/ідентифікатор; метадані; журнал операцій; хеш	Хеш подають як доказ правдивості первинного змісту
2. Змістова верифікація	Чи відповідають місце, час, зміст і переклад дійсності?	Гео- і хронолокація; повний контекст; незалежні фото, документи, свідчення	Вірусність або мітку платформи приймають за підтвердження
3. Атрибуція	Що пов'язує акаунт, номер, пристрій чи дію з особою або організацією?	Дані платформи й оператора; пристрій; реєстри; стиль; поведінкова сукупність	Контроль ідентифікатора ототожнюють з авторством
4. Юридико-контекстуальна достатність	Який елемент злочину або відповідальності підтримує матеріал?	Карта елементів; контекст; альтернативна кваліфікація; змішані джерела	Факт руху чи наказ автоматично вважають доказом складу злочину

Джерело: розроблено автором на основі [1–10; 11–21]. Набір матеріалів є індикативним і не гарантує допустимості або достатності

Таблиця 2

Юридико-контекстуальна карта доказування

Кваліфікація	Що підлягає доведенню	Релевантні цифрові джерела	Критична межа
Воєнний злочин: ст. 8(2)(a)(vii) та/або 8(2)(b)(viii)	Переміщення/депортація захищених осіб; зв'язок із міжнародним конфліктом та окупацією; відсутність дозволеного винятку	Маршрути, списки, транспортні реєстри, накази, геодані, листування	Евакуація за ст. 49 ЖК IV має вузькі умови; сам рух не доводить незаконності
Злочин проти людяності: ст. 7(1)(d)	Примусове переміщення законно присутніх осіб; поширений або систематичний напад; політика; знання	Масиви маршрутів, повторювані інструкції, бази, комунікації, публічні заяви	Примус охоплює примусове середовище, але контекст нападу й індивідуальна вина доводяться окремо
Передача дітей: ст. 6(e)	Захищена група; дитячий вік; насильницька передача до іншої групи; спеціальний намір	Реєстри опіки/усиновлення, зміни імен і статусу, програми виховання, перешкоди поверненню	Спеціальний намір знищити групу не презюмується з факту незаконного переміщення

Джерело: складено автором на основі [1, ст. 6(e), 7(1)(d), 8(2)(a)(vii), 8(2)(b)(viii); 3, с. 4–5, 7, 11; 4, ст. 49; 5, ст. 74, 78, 85(4)(b)]

ментів злочину. Її новизна полягає в локалізації доказового розриву, а не у проголошенні нового обов'язкового стандарту.

3. Воєнний злочин депортації або переміщення, злочин проти людяності за статтею 7(1)(d) та передача дітей за статтею 6(e) потребують окремих юридичних тестів. Факт руху людей не доводить автоматично незаконність, контекст нападу, спеціальний намір або вину посадової особи.

4. Матеріали щодо України підтверджують перевагу змішаних доказових сукупностей. Цифрові реєстри, відкриті джерела й супутникові дані набувають сили у поєднанні з документами, показаннями та експертизою; жоден універсальний «мінімальний пакет» не гарантує достатності.

5. Подальші дослідження мають апробувати модель на повних матеріалах завершених проваджень, оцінити міжкодувальну узгодженість і розробити сумісні протоколи для слідчих та громадських документаторів. Пріоритетними залишаються пояснюваність, рівність сторін, безпечне управління даними дітей і своєчасне збереження платформної інформації.

Список літератури:

1. Rome Statute of the International Criminal Court. 17 July 1998, as amended. International Criminal Court. URL: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf (дата звернення: 22.08.2026).

2. Rules of Procedure and Evidence. International Criminal Court, 2026. URL: https://www.icc-cpi.int/sites/default/files/2026-02/RulesProcedureEvidenceEng-2026.pdf (дата звернення: 22.08.2026).

3. Elements of Crimes. International Criminal Court, 2013. URL: https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf (дата звернення: 22.08.2026).

4. Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949. Art. 49. ICRC IHL Databases. URL: https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-49 (дата звернення: 22.08.2026).

5. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Arts. 74, 78, 85(4)(b). ICRC IHL Databases. URL: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 (дата звернення: 22.08.2026).

6. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. OHCHR; Human Rights Center, University of California, Berkeley, 2022. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 22.08.2026).

7. Aalto-Setälä S., Caroli L., Freytag J., Jaramillo Gomez M. F., Lim J. Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals. Leiden University, 2022. URL: https://leiden-guidelines.com/assets/Leiden%20Guidelines%20on%20the%20Use%20of%20DDE%20in%20ICCTs_20220404.pdf (дата звернення: 22.08.2026).

8. Eurojust, Genocide Network, Office of the Prosecutor of the International Criminal Court. Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organizations. 2022. URL: https://www.eurojust.europa.eu/sites/default/files/assets/files/eurojust-icc-csos-guidelines.pdf (дата звернення: 22.08.2026).

9. Çalı B., Finnerty J., Freeman L. et al. Evaluating Digital Open Source Imagery: A Guide for Judges and Fact-Finders. Human Rights Center, University of California, Berkeley, 2024. URL: https://humanrights.berkeley.edu/wp-content/uploads/archive/2024/05/Guide-for-judges.pdf (дата звернення: 22.08.2026).

10. Prosecutor v. Rodrigo Roa Duterte. Unified Technical Protocol for the Presentation of Evidence through the E-Court. ICC-01/21-01/25-116-Anx, 22 April 2025. URL: https://www.icc-cpi.int/court-record/icc-01/21-01/25-116 (дата звернення: 22.08.2026).

11. McDermott Y., Koenig A., Murray D. Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations. *Journal of International Criminal Justice*. 2021. Vol. 19, No. 1. P. 85–105. DOI: https://doi.org/10.1093/jicj/mqab006.

12. Gillett M., Fan W. Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom. *Journal of International Criminal Justice.* 2023. Vol. 21, No. 4. P. 661–693. DOI: https://doi.org/10.1093/jicj/mqad050.

13. de Arcos Tejerizo M. Digital Evidence and Fair Trial Rights at the International Criminal Court. Leiden Journal of International Law. 2023. Vol. 36, No. 3. P. 749–769. DOI: https://doi.org/10.1017/S0922156523000031.

14. Hamilton R. User-Generated Evidence. *Columbia Journal of Transnational Law.* 2018. Vol. 57. P. 1–61. URL: https://digitalcommons.wcl.american.edu/facsch_lawrev/1285 (дата звернення: 22.08.2026).

15. Koenig A. 'Half the Truth Is Often a Great Lie': Deep Fakes, Open Source Information, and International Criminal Law. AJIL Unbound. 2019. Vol. 113. P. 250–255. DOI: https://doi.org/10.1017/aju.2019.47.

16. Ulbricht B. R., Moxley C., Austin M. D., Norburg M. D. Digital Eyewitnesses: Using New Technologies to Authenticate Evidence in Human Rights Litigation. *Stanford Law Review.* 2022. Vol. 74. P. 851–926. URL: https://review.law.stanford.edu/wp-content/uploads/sites/3/2022/04/Ulbricht-et-al.-74-Stan.-L.-Rev.-851.pdf (дата звернення: 22.08.2026).

17. McDermott Y., Hausknecht A., Liefgreen A. New Evidence, New Challenges: ICC Judges' Perspectives on User-Generated Evidence and Judging in an Age of Artificial Intelligence. Oñati Socio-Legal Series. 2026. Advance online publication. DOI: https://doi.org/10.35295/osls.iisl.2375.

18. Lecorps Y., Naili K., Obidzinski M., Oytana Y., Toutounji T. How Is Digital Evidence Used in the International Criminal Court? An Exploratory Analysis. *European Journal of Law and Economics.* 2026. Vol. 62. P. 97–129. DOI: https://doi.org/10.1007/s10657-026-09881-3.

19. Gavrysh K. Digital Evidence in the Practice of the International Criminal Court: What Future for Proceedings on War Crimes Committed in Ukraine? In: Prosecution of War Crimes before the ICC. 2025. P. 107–129. DOI: https://doi.org/10.1007/978-3-031-84216-0_6.

20. Kuczyńska H. The ICC Interactive Digital Platform: The Power of Visual Narration and the Shifting Paradigm of Evidentiary Law. International Journal for the Semiotics of Law. 2026. Advance online publication. DOI: https://doi.org/10.1007/s11196-026-10534-6.

21. Prosecutor v. Jean-Pierre Bemba Gombo. Judgment on the Appeals of Mr Jean-Pierre Bemba Gombo and the Prosecutor against the Decision of Trial Chamber III Entitled 'Decision on the Admission into Evidence of Materials Contained in the Prosecution's List of Evidence'. ICC-01/05-01/08-1386, 3 May 2011. URL: https://www.icc-cpi.int/court-record/icc-01/05-01/08-1386 (дата звернення: 22.08.2026).

22. Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli. Warrant of Arrest. ICC-01/11-01/17-2, 15 August 2017. URL: https://www.icc-cpi.int/court-record/icc-01/11-01/17-2 (дата звернення: 22.08.2026).

23. Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud. Trial Judgment. ICC-01/12-01/18-2594-Red, 26 June 2024. URL: https://www.icc-cpi.int/court-record/icc-01/12-01/18-2594-red (дата звернення: 22.08.2026).

24. Prosecutor v. Alfred Yekatom and Patrice-Edouard Ngaïssona. Judgment. ICC-01/14-01/18-2784-Red, 24 July 2025. URL: https://www.icc-cpi.int/court-record/icc-01/14-01/18-2784-red (дата звернення: 22.08.2026).

25. Prosecutor v. Alfred Yekatom and Patrice-Edouard Ngaïssona. Yekatom Defence Notice of Appeal. ICC-01/14-01/18-2815, 26 September 2025. URL: https://www.icc-cpi.int/court-record/icc-01/14-01/18-2815 (дата звернення: 22.08.2026).

26. Situation in Ukraine: ICC Judges Issue Arrest Warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova. International Criminal Court. 17 March 2023. URL: https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and (дата звернення: 22.08.2026).

27. Moscow Mechanism: Report on Violations and Abuses of International Humanitarian and Human Rights Law, War Crimes and Crimes against Humanity, Related to the Forcible Transfer and/or Deportation of Ukrainian Children to the Russian Federation. OSCE/ODIHR, 4 May 2023. URL: https://odihr.osce.org/odihr/542751 (дата звернення: 22.08.2026).

28. Ukraine and the Netherlands v. Russia [GC], applications nos. 8019/16, 43800/14, 28525/20 and 11055/22, Judgment (Merits), 9 July 2025. HUDOC. URL: https://hudoc.echr.coe.int/?i=001-244292 (дата звернення: 22.08.2026).

29. Independent International Commission of Inquiry on Ukraine. 'I Am Still Looking for My Daughter': Crimes against Humanity Committed by Russian Authorities against Children from Ukraine. A/HRC/61/CRP.8, 9 March 2026. URL: https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session61/a-hrc-61-crp-8.pdf (дата звернення: 22.08.2026).

30. Office of the United Nations High Commissioner for Human Rights. Forced Displacement from Territory of Ukraine Occupied by the Russian Federation. 20 March 2026. URL: https://ukraine.ohchr.org/sites/default/files/2026-03/2026-03-20%20OHCHR%20-%20Thematic%20report%20-%20Forced%20displacement.pdf (дата звернення: 22.08.2026).

31. Raymond N. A., Hathaway O. A., Howarth C. N., Khoshnood K. et al. Intentional, Systematic, & Widespread: Russia's Program of Coerced Adoption and Fostering of Ukraine's Children. Yale Humanitarian Research Lab, 2024. URL: https://medicine.yale.edu/news-article/russias-systematic-program-of-coerced-adoption-and-fostering-of-ukraines-children (дата звернення: 22.08.2026).

32. Starling Lab. New Evidence Techniques Document Bombed Ukrainian Schools for the ICC: Case Study. URL: https://starlinglab.org/case-studies/submission-icc-schools-kharkiv-evidence-case-study (дата звернення: 22.08.2026).

Semenov S. V., Adamovsky V. I. DIGITAL EVIDENCE STANDARDS IN INTERNATIONAL CRIMINAL LAW: A FOUR-LEVEL MODEL FOR CASES INVOLVING THE DEPORTATION AND FORCIBLE TRANSFER OF UKRAINIAN CIVILIANS

This article examines standards for collecting, preserving, verifying, presenting and assessing digital evidence in international criminal law and adapts them to proceedings concerning the deportation and forcible transfer of Ukrainian civilians. Based on a structured doctrinal and comparative analysis of the Rome Statute, the ICC Rules of Procedure and Evidence, the Elements of Crimes, relevant ICC practice, soft-law instruments and materials produced by international mechanisms concerning Ukraine, the article clarifies the limits of the Court's technology-neutral free-evaluation model. It distinguishes digital evidence, digitally derived evidence, digital open source information and user-generated evidence. It shows that technical file integrity does not establish the truth of content, while identifying an account, number or device does not automatically establish authorship or criminal responsibility. A four-level verification model is proposed:

(1) provenance and integrity; (2) content verification; (3) attribution; and (4) legal-contextual sufficiency. Rather than a universal technical standard, the model integrates existing verification procedures with separate legal tests for the war crime of unlawful deportation or transfer, the crime against humanity of deportation or forcible transfer, and the forcible transfer of children as conduct under Article 6(e) of the Rome Statute. The model is tested against Al-Werfalli, Al Hassan, Yekatom and Ngaïssona and the Ukraine-related evidentiary record published in 2023–2026. Evidentiary strength emerges from the convergence of verified and, where possible, independent digital, documentary, testimonial and expert sources. No universal "minimum package" guarantees admissibility or sufficiency outside the context of a specific charge.

Keywords: *digital evidence, digital open source information, OSINT, international criminal law, deportation, forcible transfer, International Criminal Court, authentication, attribution, children's rights.*

Дата першого надходження статті до видання: 04.09.2026
Дата прийняття статті до друку після рецензування: 18.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026