УДК 343.85:343.541
DOI https://doi.org/10.32782/2307-1745.2026.83.32

Ричка Д. О.,
кандидат юридичних наук,
доцент кафедри правоохоронної діяльності
Університету митної справи та фінансів
ORCID: https://orcid.org/0009-0001-0207-907X

Скачедуб С. А.,
старший викладач кафедри публічного управління та права
ННІ Придніпровська державна академія
будівництва та архітектури
Українського державного університету науки та технології
ORCID: https://orcid.org/0000-0002-4256-1127

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПРАВООХОРОННИХ ОРГАНІВ ЩОДО ПРОТИДІЇ ПОРУШЕННЯМ ПРАВ ДИТИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ ТА МЕХАНІЗМИ ЙОГО ВДОСКОНАЛЕННЯ

Анотація. У статті досліджено міжнародне співробітництво правоохоронних органів у сфері протидії порушенням прав дитини у цифровому середовищі, зокрема у випадках секстингу, кібергрумінгу, сексуальної експлуатації дітей, поширення матеріалів сексуального насильства над дітьми та інших форм технологічно опосередкованого сексуального насильства.

Цифрове середовище змінило традиційні межі кримінально-правового реагування, оскільки злочинець, потерпіла дитина, цифрова платформа, сервер, платіжний інструмент, електронні докази та юрисдикція можуть перебувати у різних державах. У таких умовах ефективний захист дитини неможливий без швидкого міжнародного обміну даними, використання каналів Інтерполу, Європолу, мережі постійно діючих контактних пунктів за Будапештською конвенцією, міжнародних баз ідентифікації жертв, механізмів збереження електронних доказів та співпраці з приватними цифровими платформами.

Проаналізовано трирічний горизонт 2023–2025 років, у межах якого виокремлено три ключові тенденції: зростання масштабів повідомлень про онлайн-сексуальну експлуатацію дітей; посилення ролі платформних даних, гарячих ліній і міжнародних баз даних; поява нових ризиків, пов'язаних із генеративним штучним інтелектом, шифрованими сервісами, фінансовим сексторшеном і транскордонним обігом матеріалів сексуального насильства над дітьми.

Звернуто увагу на міжнародні приклади, зокрема операцію Europol щодо платформи Kidflix, операції Інтерполу щодо виявлення жертв і підозрюваних у різних юрисдикціях, а також український портал StopCrime як інструмент повідомлення про сексуальне насильство над дітьми онлайн.

Окремо розглянуто суміжні теми, які вже вивчалися українськими науковцями, а саме цифрові права дітей, міжнародний досвід протидії сексуальній експлуатації дітей в Інтернеті, міжнародне співробітництво у сфері боротьби з кіберзлочинністю, застосування штучного інтелекту для протидії злочинам у сфері сексуальної експлуатації дітей.

Запропоновано механізми вдосконалення: створення спеціалізованої національної моделі міжнародної взаємодії у справах про онлайн-насильство щодо дітей; посилення постійно-діючого контактного пункту; запровадження стандарту невідкладного збереження цифрових доказів; розвиток співпраці з INHOPE, NCMEC, Інтерполом та Європолом; формування національного протоколу взаємодії між Кіберполіцією, органами прокуратури, ювенальною поліцією, Мінцифрою, соціальними службами та закладами освіти.

Ключові слова: права дитини, цифрове середовище, онлайн-безпека дітей, секстинг, кібергрумінг, сексуальне насильство щодо дітей, сексуальна експлуатація дітей, дитяча порнографія та/або матеріали сексуального насильства над дітьми, нормативно-правові інструменти, дитиноцентричне правосуддя.

Постановка проблеми. Цифрове середовище є одним із ключових просторів реалізації прав дитини – права на освіту, інформацію, комунікацію, участь у суспільному житті, творчість і самовираження [1]. Водночас воно стало простором підвищеної уразливості, оскільки дитина може взаємодіяти з невідомими особами, алгоритмічно рекомендованим контентом, закритими групами, шифрованими каналами комунікації, онлайн-іграми, соціальними мережами та платформами для обміну зображеннями [1; 5; 6; 10].

Загальний коментар № 25 Комітету ООН з прав дитини підкреслює, що права дитини мають повністю поважатися, захищатися й реалізовуватися також у цифровому середовищі, а держави повинні адаптувати законодавство та інституційну практику до технологічних змін [1].

Особливістю порушень прав дитини у цифровому середовищі є їхня транскордонність. У кримінальному провадженні щодо кібергрумінгу, сексуального шантажу або поширення матеріалів сексуального насильства над дітьми слідчий може стикнутися з ситуацією, коли потерпіла дитина перебуває в Україні, підо-

зрюваний – в іншій державі, сервер – у третій, платіжний рахунок – у четвертій, а цифрова платформа належить компанії, зареєстрованій взагалі поза межами Європи [3; 4; 11]. Саме тому класична модель внутрішньодержавного розслідування є недостатньою.

Необхідною стає модель міжнародного правоохоронного співробітництва, яка поєднує кримінально-процесуальні інструменти, оперативний обмін інформацією, технічну ідентифікацію жертв, співпрацю з онлайн-платформами та дитиноцентричні механізми захисту [2; 3; 4; 11; 12; 13].

Упродовж 2023–2025 років ця проблема набула особливої актуальності. NCMEC повідомляв, що у 2023 році CyberTipline отримала понад 36,2 млн повідомлень про підозрювану сексуальну експлуатацію дітей онлайн, а кількість повідомлень про онлайн-спокушання, включно із сексторшеном, зросла більш ніж на 300% порівняно з 2021 роком [8].

У 2024 році загальна кількість повідомлень CyberTipline зменшилася до 20,5 млн, однак NCMEC пов'язував це не з вирішенням проблеми, а зі змінами у структурі звітування та одночасним зростанням окремих категорій повідомлень [9].

У 2025 році WeProtect Global Alliance прямо зазначила, що масштаб і складність технологічно опосередкованої сексуальної експлуатації та насильства над дітьми випереджають наявні глобальні механізми захисту [10].

Аналіз останніх досліджень і публікацій. Українська наукова думка вже сформувала низку суміжних напрямів, на які доцільно спиратися при дослідженні міжнародного співробітництва правоохоронних органів щодо захисту дітей у цифровому середовищі [16; 17; 18; 19; 20].

По-перше, вивчається загальна проблематика цифрових прав дітей. Зокрема, Л.А. Музика у статті «Цифрові права дітей: сучасні виклики та євроінтеграція» досліджує правове регулювання цифрових прав дитини, їх види, проблеми правового регулювання та практики застосування, акцентуючи увагу на захисті персональних даних, протидії кіберзлочинності та євроінтеграційному контексті [16]. Цей напрям є важливим для цієї статті, оскільки міжнародне поліцейське співробітництво не може розглядатися лише як інструмент репресії; воно має бути підпорядковане правам дитини, принципу найкращих інтересів дитини та стандартам захисту персональних даних [1; 16].

По-друге, українські дослідники аналізували міжнародний досвід протидії сексуальній експлуатації дітей в Інтернеті. В. Сенько у праці «Актуальні питання протидії сексуальній експлуатації дітей та сексуального насильства над дітьми в інтернеті: міжнародний досвід» розглядав зарубіжні підходи до протидії таким діянням, у тому числі значення баз даних, міждержавної взаємодії та співпраці з приватним сектором [17].

По-третє, значний блок українських публікацій стосується міжнародного співробітництва у сфері протидії кіберзлочинності загалом.

М.В. Гуцалюк аналізував напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю, а А.В. Войціховський ще раніше звертав увагу на комплекс проблем міжнародної співпраці правоохоронних органів у боротьбі з кіберзлочинністю [18; 19].

Ці праці створюють загальну методологічну основу для теми, однак потребують спеціалізації саме на злочинах проти дітей у цифровому середовищі [18; 19].

По-четверте, у 2025 році з'являються дослідження щодо застосування штучного інтелекту для протидії злочинам у сфері сексуальної експлуатації дітей у мережі Інтернет. О.І. Зачек аналізує можливості використання ШІ для протидії таким злочинам, що є особливо актуальним у контексті автоматизованого виявлення CSAM, ідентифікації повторюваних матеріалів, аналізу великих масивів даних і пошуку цифрових слідів [20].

Отже, в передовій українській науці вже розглядаються цифрові права дитини, сексуальна експлуатація дітей онлайн, міжнародне співробітництво у боротьбі з кіберзлочинністю та використання ШІ для протидії відповідним злочинам [16; 17; 18; 19; 20].

Водночас недостатньо розробленою залишається саме комплексна модель міжнародного співробітництва правоохоронних органів у справах про порушення прав дитини у цифровому середовищі, яка поєднувала б кримінальний процес, оперативну взаємодію, платформну відповідальність, захист персональних даних, дитиноцентричне правосуддя та реабілітацію потерпілої дитини [1; 5; 6; 11; 16; 20].

Мета статті. Метою статті є комплексний аналіз міжнародного співробітництва правоохоронних органів щодо протидії порушенням прав дитини у цифровому середовищі, визначення проблем чинної моделі такої взаємодії та обґрунтування механізмів її вдосконалення з урахуванням міжнародно-правових інструментів, практики Інтерполу, Європолу, міжнародних мереж і цифрових платформ, а також дитиноцентричного підходу.

Виклад основного матеріалу. Базовим міжнародним документом у сфері протидії сексуальній експлуатації та сексуальному насильству щодо дітей є Ланцаротська конвенція [2]. Вона визначає комплексний підхід до захисту дітей, охоплюючи запобігання сексуальному насильству, криміналізацію відповідних діянь, захист дітей-жертв і міжнародне співробітництво [2]. Рада Європи характеризує Ланцаротську конвенцію як комплексний міжнародний правовий інструмент захисту дітей від сексуальної експлуатації та сексуального насильства [2].

Другим ключовим документом є Конвенція про кіберзлочинність, або Будапештська конвенція [3]. Для цієї теми вона має подвійне значення. По-перше, її стаття 9 стосується правопорушень, пов'язаних із дитячою порнографією, вчинених із використанням комп'ютерних систем [3]. По-друге, Конвенція створює процесуальну й інституційну основу для міжнародної взаємодії, зокрема через мережу постійно-діючих контактних пунктів, які мають забезпечувати невідкладну допомогу у справах, пов'язаних із комп'ютерними даними та електронними доказами [3; 4].

Для України важливим є те, що Будапештська конвенція є чинною для України з 2006 року. Офіційна база Верховної Ради України зазначає, що документ ратифіковано Україною, а набрання чинності для України відбулося 01.07.2006 [3]. В умовах цифрових злочинів проти дітей це означає, що Україна має не лише формальну договірну базу для міжнародної взаємодії, а й практичний обов'язок підтримувати дієвий механізм швидкого обміну даними, збереження електронних доказів і комунікації з іноземними компетентними органами [3; 4].

На рівні Європейського Союзу важливе значення має Digital Services Act. Регламент (EU) 2022/2065 встановлює правила відповідальності цифрових послуг і платформ, а стаття 28 передбачає спеціальний захист неповнолітніх на онлайн-платформах [5]. У 2025 році Європейська комісія опублікувала керівні

принципи щодо заходів для забезпечення високого рівня приватності, безпеки й захисту неповнолітніх онлайн відповідно до статті 28(4) DSA [6].

В українському законодавстві важливими є зміни, внесені Законом України «Про внесення змін до деяких законодавчих актів України щодо імплементації Ланцаротської конвенції» від 18 лютого 2021 року щодо імплементації Ланцаротської конвенції [7]. Цей Закон став підставою для оновлення кримінально-правового реагування на сексуальні злочини проти дітей, зокрема для появи норм про домагання дитини для сексуальних цілей та спеціальних складів щодо дитячої порнографії [7].

У межах цієї статті проаналізовано трирічний горизонт 2023–2025 роки, тобто останній повний трирічний період, який дозволяє простежити сталі тенденції до початку 2026 року. Окремі події 2026 року можуть використовуватися як підтвердження тенденцій, започаткованих у 2025 році [8; 9; 10].

2.1. 2023 рік: різке зростання повідомлень і проблема доказового перевантаження. У 2023 році NCMEC повідомив про понад 36,2 млн повідомлень до CyberTipline та понад 105 млн файлів, пов'язаних із підозрюваною сексуальною експлуатацією дітей. Також було зафіксовано 186 819 повідомлень про онлайн-спокушання, включно із сексторшеном [8].

Ці дані демонструють головну проблему міжнародного співробітництва: правоохоронні органи дедалі частіше працюють не з одиничними епізодами, а з великими масивами повідомлень, зображень, відео, чатів, IP-адрес, акаунтів, платіжних слідів і метаданих [8; 10; 11]. Тому ефективність співробітництва залежить не лише від наявності міжнародного договору, а й від технічної сумісності баз даних, якості повідомлень від платформ, швидкості збереження доказів і здатності відокремити пріоритетні загрози від масового інформаційного шуму [3; 4; 8; 11].

2.2. 2024 рік: інституційне посилення повідомлень і запуск українського StopCrime. У 2024 році в Україні запрацював портал StopCrime – перший портал повідомлень про матеріали, пов'язані із сексуальним насильством над дітьми в мережі [14]. Міністерство цифрової трансформації України зазначало, що повідомлення може бути анонімним, а головне – надати посилання, де розміщено відповідний контент; ГО «Магнолія», як член міжнародної мережі INHOPE збирає, аналізує та передає інформацію до Кіберполіції та Інтерполу [14].

Національна поліція України у вересні 2024 року повідомила, що з початку року за допомогою StopCrime було верифіковано 687 повідомлень про сексуальне насильство над дітьми, а інформація про такі факти передавалася до правоохоронних органів країн за місцем імовірного вчинення злочинів [15].

Це важливий приклад не лише національного, а й транскордонного механізму, оскільки повідомлення громадян можуть стосуватися контенту, розміщеного за межами України, або матеріалів, пов'язаних з іноземними цифровими сервісами [14; 15].

2.3. 2025 рік: платформна відповідальність, ШІ та масштабні міжнародні операції. У 2025 році європейський підхід до захисту дітей онлайн дедалі більше зміщується від моделі реагування на вже виявлений незаконний контент до моделі превентивного управління ризиками платформ [5; 6].

Публікація керівних принципів Європейської комісії щодо захисту неповнолітніх за DSA свідчить про формування нового стандарту: платформа має не лише видаляти незаконний контент, а й проєктувати свої сервіси так, щоб зменшувати ризики грумінгу, небажаних контактів, сексуалізованого контенту, маніпулятивних інтерфейсів і шкідливих алгоритмічних рекомендацій [6].

Паралельно WeProtect Global Alliance у Global Threat Assessment 2025 звернула увагу на те, що технологічно опосередкована сексуальна експлуатація дітей прискорюється через шифровані простори, фінансовий сексторшен, генеративний ШІ та взаємоперетин різних форм шкоди [10].

Це означає, що міжнародне співробітництво правоохоронних органів має враховувати не лише класичні форми обміну доказами, а й нові інструменти: аналіз синтетичних зображень, виявлення фінансових потоків, швидке блокування токенізованих або криптовалютних платежів, співпрацю з провайдерами генеративних моделей і платформами обміну контентом [10; 20].

2.4. Приклади міжнародного співробітництва правоохоронних органів. Одним із найбільш показових прикладів є міжнародна операція проти платформи Kidflix. Europol повідомив, що в операції брали участь понад 35 країн; було арештовано 79 підозрюваних, вилучено понад 3 000 електронних пристроїв, захищено 39 дітей, а сама платформа містила понад 91 000 відео з матеріалами сексуального насильства над дітьми [12].

Цей приклад демонструє кілька важливих висновків. По-перше, сучасні злочини проти дітей у цифровому середовищі часто мають платформну організацію, тобто йдеться не лише про окремого користувача, а про інфраструктуру обігу незаконного контенту [12]. По-друге, криптовалютні або токенізовані механізми оплати можуть використовуватися для підтримання такої інфраструктури [12]. По-третє, успішне припинення діяльності подібної платформи потребує синхронізованих дій кількох держав, одночасного вилучення серверів, ідентифікації адміністраторів, користувачів і потерпілих дітей [11; 12].

У 2025 році Інтерпол повідомив про міжнародну операцію проти виробництва та розповсюдження матеріалів сексуального насильства над дітьми, яку ініціювала іспанська поліція за участю Інтерполу та Європолу [13]. У результаті було заарештовано 20 осіб у 12 країнах Америки та Європи; підставою стали онлайн-групи в месенджерах, де поширювалися зображення сексуальної експлуатації дітей [13].

Цей приклад цікавий тим, що демонструє значення не лише формальних запитів про міжнародну правову допомогу, а й робочих зустрічей, спеціалізованих груп з ідентифікації жертв і оперативного обміну орієнтуваннями [11; 13].

У справах про дітей час має критичне значення: чим швидше встановлено країну перебування дитини, платформу, акаунт або підозрюваного, тим вищі шанси припинити насильство та зберегти докази [4; 11; 13].

Український StopCrime є важливим прикладом гібридної моделі, де поєднуються зусилля держави, громадських організацій, міжнародної мережі гарячих ліній і правоохоронних органів [14; 15].

Створено проєкт ГО «Магнолія» за підтримки Міністерства цифрової трансформації, Дія.Освіта та Департаменту кіберполіції Національної поліції України, ГО «Магнолія» є членом INHOPE [14].

Особлива цінність цієї моделі полягає у тому, що вона дає громадянам простий канал повідомлення про матеріали сексуального насильства над дітьми онлайн, а правоохоронним органам – структурований потік інформації, який може бути використаний для блокування контенту, ідентифікації серверів,

встановлення країни походження матеріалу та передачі інформації іноземним компетентним органам [14; 15].

2.5. Проблеми чинної моделі міжнародного співробітництва. Незважаючи на наявність міжнародно-правових інструментів, чинна модель співробітництва має низку проблем [2; 3; 4; 10; 11].

Перша проблема – часова невідповідність між швидкістю цифрового злочину та швидкістю правової допомоги. Матеріали сексуального насильства над дітьми можуть поширюватися за хвилини, тоді як класичні запити про міжнародну правову допомогу можуть опрацьовуватися тижнями або місяцями [3; 4; 10]. Саме тому важливо розвивати не лише MLAT-процедури, а й механізми невідкладного збереження даних, постійно-діючі контактні пункти і попередній оперативний обмін інформацією [3; 4].

Друга проблема – залежність від приватних платформ. У багатьох провадженнях ключові дані перебувають у розпорядженні соціальних мереж, месенджерів, хостинг-провайдерів, хмарних сервісів, платіжних систем або платформ для обміну файлами [5; 6; 8; 10]. Без швидкої комунікації з ними правоохоронні органи можуть втратити IP-адреси, журнали входів, дані акаунтів, хеші файлів або листування [3; 4; 5; 6].

Третя проблема – шифрування та анонімізація. Шифровані канали самі по собі є важливим інструментом захисту приватності, однак вони також можуть використовуватися правопорушниками для приховування кібергрумінгу, сексторшену, обміну CSAM і координації злочинної діяльності [10]. WeProtect Global Alliance визначає шифровані простори одним із факторів, що ускладнюють глобальну протидію сексуальній експлуатації дітей онлайн [10].

Четверта проблема – ризик вторинної віктимізації дитини. Міжнародне співробітництво не повинно перетворювати дитину на «джерело доказів», яке багаторазово опитують різні органи [1; 2]. Дитиноцентричний підхід вимагає мінімізації повторних допитів, конфіденційності, психологічної підтримки, захисту від контакту з кривдником і швидкого видалення незаконного контенту [1; 2; 14; 15].

П'ята проблема – відсутність достатньо деталізованої статистики. Україна потребує системи, яка окремо відображатиме кількість проваджень щодо кібергрумінгу, сексторшену, поширення CSAM, використання ШІ для створення сексуалізованих зображень дітей, міжнародних запитів, звернень до платформ, відповідей іноземних органів і випадків ідентифікації потерпілих дітей [8; 9; 10; 11; 20].

2.6. Механізми вдосконалення міжнародного співробітництва. Доцільно розробити спеціальний міжвідомчий протокол дій у справах про онлайн-сексуальне насильство щодо дітей [1; 2; 3; 4; 14; 15].

Він має визначати порядок взаємодії Кіберполіції, ювенальної превенції, слідчих органів, прокуратури, Мінцифри, соціальних служб, освітніх закладів, гарячих ліній і міжнародних партнерів [14; 15].

Такий протокол має передбачати:

1. Первинну оцінку ризику для дитини;
2. Невідкладне збереження цифрових доказів;
3. Визначення юрисдикції сервера, платформи або підозрюваного;
4. Звернення через постійно-діючий контактний пункт;
5. Передачу інформації до Інтерполу або Європолу;
6. Взаємодію з INHOPE, NCMEC та іншими гарячими лініями;
7. Забезпечення психологічного й правового супроводу дитини;
8. Процедуру екстреного видалення або обмеження доступу до матеріалів [3; 4; 8; 11; 12; 13; 14; 15].

Мережа постійно-діючих контактних пунктів за Будапештською конвенцією має бути одним із ключових інструментів у справах щодо дітей [3; 4]. Рада Європи прямо зазначає, що підтримує функціонування мережі постійно-діючих контактних пунктів відповідно до статті 35 Конвенції про кіберзлочинність, зокрема шляхом ведення каталогу контактних пунктів [4].

Для України доцільно передбачити спеціалізацію в межах контактного пункту саме щодо злочинів проти дітей у цифровому середовищі [3; 4]. Це означає, що чергові фахівці мають бути підготовлені не лише з технічних питань кіберзлочинності, а й з питань захисту дітей, термінології CSAM, взаємодії з платформами, пріоритизації випадків, де дитина може перебувати в актуальній небезпеці [1; 3; 4; 11].

Україна підписала Другий додатковий протокол до Будапештської конвенції у 2022 році разом із Республікою Молдова; Рада Європи зазначала, що його підписання відкриває можливості для вдосконалення міжнародного співробітництва щодо кіберзлочинності та електронних доказів [3; 4].

У 2025 році Рада Європи та Eurojust проводили для України захід, присвячений операційним і правовим наслідкам цього Протоколу, який передбачає нові форми прямої співпраці з постачальниками послуг, прискорені процедури запитів даних і посилені гарантії прав людини [3; 4].

Для справ про дітей це має принципове значення. Найбільш цінні докази – IP-адреси, журнали входу, дані акаунтів, метадані, інформація про пристрої, платіжні сліди – можуть бути швидко видалені або змінені [3; 4; 8; 10]. Тому Україна має розглядати імплементацію таких процедур як один із пріоритетів кримінальної юстиції у цифровому середовищі [3; 4].

Міжнародна база даних сексуальної експлуатації дітей є одним із ключових інструментів міжнародної ідентифікації дітей-жертв [11]. Інтерпол повідомляє, що ця база містить 4,9 млн зображень і відео та допомогла ідентифікувати 42 300 жертв у світі; доступ до неї мають спеціалізовані слідчі більш ніж із 70 країн [11].

Україні доцільно посилювати підготовку спеціалістів, які працюють з такими базами, оскільки у справах про CSAM правоохоронець часто починає не з заяви потерпілої дитини, а з цифрового зображення, відео або фрагмента локації [11]. Саме тому потрібні навички OSINT-аналізу, візуальної ідентифікації, геолокації, аналізу метаданих, порівняння хешів і співставлення з міжнародними базами [11; 18; 20].

Також Україні доцільно адаптувати окремі елементи європейської моделі DSA [5; 6]. Йдеться не про механічне копіювання, а про поступове формування національної моделі платформної відповідальності щодо дітей [5; 6].

Онлайн-платформи, доступні дітям, повинні мати обов'язки щодо:

– швидкого реагування на повідомлення про CSAM;

– збереження доказів для правоохоронних органів;

– блокування повторного завантаження відомих незаконних матеріалів;

– обмеження небажаних контактів дорослих із дітьми;

– прозорої системи скарг;

– співпраці з довіреними повідомниками;

– звітності щодо видалення матеріалів сексуального насильства над дітьми [5; 6; 8; 10].

Європейські керівні принципи за DSA у 2025 році підтверджують, що безпека дітей має бути інтегрована у саму архітектуру онлайн-платформ, а не лише в процедури реагування після скарги [6].

Штучний інтелект також може бути використаний для ідентифікації повторюваних матеріалів, класифікації ризиків, пошуку зв'язків між акаунтами, аналізу відкритих джерел, виявлення патернів грумінгу та прискорення обробки великих масивів повідомлень [20].

Водночас використання ШІ в цій сфері потребує процесуальних гарантій: перевірюваності результатів, людського контролю, захисту персональних даних, недопущення автоматичного прийняття процесуальних рішень без оцінки слідчого або прокурора [1; 20].

Це важливо і з огляду на те, що генеративний ШІ сам стає інструментом створення синтетичних сексуалізованих матеріалів за участю дітей або зображень осіб, які виглядають як діти [10; 20].

NCMEC у 2026 році повідомляв, що у 2025 році отримав понад 1,5 млн повідомлень CyberTipline, які мали зв'язок із генеративним ШІ та сексуальною експлуатацією дітей [8; 9; 20].

Висновки. Міжнародне співробітництво правоохоронних органів у сфері протидії порушенням прав дитини у цифровому середовищі є об'єктивною необхідністю, а не факультативним елементом кримінального провадження [1; 2; 3; 4]. Транскордонна природа кібергрумінгу, сексторшену, поширення матеріалів сексуального насильства над дітьми, використання цифрових платформ, хмарних сервісів, шифрованих месенджерів і платіжних інструментів робить неможливою ефективну протидію виключно національними засобами [3; 4; 5; 8; 10; 11].

Аналіз 2023–2025 років показує, що проблема має тенденцію до ускладнення [8; 9; 10]. Зростають обсяги повідомлень, посилюється роль платформних даних, збільшується значення міжнародних баз ідентифікації жертв, а генеративний ШІ створює нові виклики для кримінального права, кримінального процесу та міжнародної взаємодії [8; 9; 10; 11; 20].

Приклади Kidflix, операцій Інтерполу та українського StopCrime демонструють, що ефективною є не ізольована діяльність окремого органу, а мережна модель: правоохоронні органи – міжнародні організації – приватні платформи – гарячі лінії – громадський сектор – соціальні служби [12; 13; 14; 15].

Для України першочерговими напрямами вдосконалення є: посилення спеціалізованого постійно-діючого контактного пункту; розроблення міжвідомчого протоколу міжнародної взаємодії у справах про онлайн-насильство щодо дітей; імплементація прискорених процедур доступу до електронних доказів; розвиток співпраці з Інтерполом, Європолом, INHOPE і NCMEC; нормативне врегулювання обов'язків платформ; підготовка спеціалізованих слідчих, прокурорів і суддів; впровадження ШІ-інструментів із правовими гарантіями; створення статистичної системи моніторингу порушень прав дитини у цифровому середовищі [3; 4; 5; 6; 8; 11; 12; 13; 14; 15; 20].

Головним принципом має залишатися дитиноцентричність [1; 2]. Міжнародне співробітництво у таких справах повинно бути спрямоване не лише на встановлення і покарання винних, а й на швидке припинення насильства, видалення незаконного контенту, ідентифікацію та захист потерпілої дитини, запобігання повторній віктимізації та відновлення порушених прав [1; 2; 11; 14; 15].

Література:

1. General comment No. 25 on children's rights in relation to the digital environment / UN Committee on the Rights of the Child. 2021. URL: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (дата звернення: 26.05.2026).
2. The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse – Lanzarote Convention / Council of Europe. URL: https://www.coe.int/en/web/gender-matters/the-council-of-europe-convention-on-the-protection-of-children-against-sexual-exploitation-and-sexual-abuse-also-known-as-the-lanzarote-convention (дата звернення: 26.05.2026).
3. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001. URL: https://zakon.rada.gov.ua/go/994_575 (дата звернення: 26.05.2026).
4. 24/7 Network established under the Convention on Cybercrime / Council of Europe. URL: https://www.coe.int/en/web/cybercrime/24/7-network-new (дата звернення: 26.05.2026).
5. Regulation (EU) 2022/2065 on a Single Market for Digital Services – Digital Services Act : Regulation of the European Parliament and of the Council of 19 October 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата звернення: 26.05.2026).
6. Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065 / European Commission. 2025. URL: https://eur-lex.europa.eu/eli/C/2025/5519/oj/eng (дата звернення: 26.05.2026).
7. Про внесення змін до деяких законодавчих актів України щодо імплементації Ланцаротської конвенції : Закон України від 18.02.2021 № 1256-IX. URL: https://zakon.rada.gov.ua/go/1256-20 (дата звернення: 26.05.2026).
8. CyberTipline Data / National Center for Missing & Exploited Children. URL: https://www.missingkids.org/gethelpnow/cybertipline (дата звернення: 26.05.2026).
9. NCMEC Releases New Data: 2024 in Numbers / National Center for Missing & Exploited Children. 2025. URL: https://www.missingkids.org/blog/2025/ncmec-releases-new-data-2024-in-numbers (дата звернення: 26.05.2026).
10. Global Threat Assessment 2025 / WeProtect Global Alliance. 2025. URL: https://www.weprotect.org/global-threat-assessment-25/ (дата звернення: 26.05.2026).
11. International Child Sexual Exploitation database / INTERPOL. URL: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (дата звернення: 26.05.2026).
12. Global crackdown on Kidflix, a major child sexual exploitation platform / Europol. 2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users (дата звернення: 26.05.2026).
13. 20 arrested in international operation targeting child sexual abuse material / INTERPOL. 2025. URL: https://www.interpol.int/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material (дата звернення: 26.05.2026).
14. Повідомляйте про сексуальне насильство над дітьми онлайн: портал StopCrime / Міністерство цифрової трансформації України. 2024. URL: https://thedigital.gov.ua/news/technologies/povidomlyayte-pro-seksualne-nasilstvo-nad-ditmi-onlayn-portal-stopcrime (дата звернення: 26.05.2026).

15. Безпека неповнолітніх: кіберполіція розвиває міжнародну співпрацю з питань захисту дітей / Національна поліція України. 2024. URL: https://npu.gov.ua/news/bezpeka-nepovnolitnikh-kiberpolitsiia-rozvyvaie-mizhnarodnu-spivpratsiu-z-pytan-zakhystu-ditei (дата звернення: 26.05.2026).
16. Музика Л. А. Цифрові права дітей: сучасні виклики та євроінтеграція. 2025. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/59.pdf (дата звернення: 26.05.2026).
17. Сенько В. Актуальні питання протидії сексуальній експлуатації дітей та сексуального насильства над дітьми в інтернеті: міжнародний досвід. 2021. URL: https://er.dduvs.edu.ua/handle/123456789/8272 (дата звернення: 26.05.2026).
18. Гуцалюк М. В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. 2021. URL: https://il.ippi.org.ua/article/view/248840 (дата звернення: 26.05.2026).
19. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. 2011. URL: https://dspace.univd.edu.ua/bitstreams/70821933-3b8f-491e-8c7f-3b2c4576d2b4/download (дата звернення: 26.05.2026).
20. Зачек О. І. Застосування штучного інтелекту для протидії злочинам у сфері сексуальної експлуатації дітей у мережі Інтернет. 2025. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/1012 (дата звернення: 26.05.2026).

Rychka D., Skachedub S. International cooperation of law enforcement agencies in combating violations of children's rights in the digital environment and mechanisms for its improvement

Summary. The article examines international cooperation between law enforcement agencies in countering violations of children's rights in the digital environment, particularly in cases of sexting, cyber grooming, child sexual exploitation, dissemination of child sexual abuse material and other forms of technology-facilitated sexual violence against children.

It is argued that the digital environment has transformed traditional criminal justice boundaries, since the offender, the child victim, the digital platform, servers, payment instruments, electronic evidence and jurisdiction may be located in different states. Under such conditions, effective child protection is impossible without rapid international data exchange, the use of INTERPOL and Europol channels, the 24/7 contact point network under the Budapest Convention, international victim identification databases, mechanisms for the preservation of electronic evidence and cooperation with private digital platforms.

The article analyses the three-year period of 2023–2025 and identifies key trends: the growing scale of reports on online child sexual exploitation; the increasing role of platform data, hotlines and international databases; and new risks associated with generative artificial intelligence, encrypted services, financial sextortion and cross-border circulation of child sexual abuse material.

The article considers practical examples, including Europol's operation against the Kidflix platform, INTERPOL operations aimed at identifying victims and suspects across jurisdictions, and Ukraine's StopCrime portal as a mechanism for reporting online child sexual abuse.

Key words: children's rights, digital environment, online child safety, sexting, cyber grooming, sexual violence against children, sexual exploitation of children, child pornography / child sexual abuse material, legal and regulatory instruments, child-centred justice.

Використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту не використовувалися.

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Дата першого надходження статті до видання: 24.08.2026
Дата прийняття статті до друку після рецензування: 19.09.2026
Дата публікації (оприлюднення) статті: 09.11.2026