

конвенційного права на вибір адвоката та підвищення ефективності правозахисту, необхідно доповнити статтю 25 Закону України «Про адвокатуру та адвокатську діяльність» [4] відповідною нормою щодо легалізації та підтримки допомоги *pro bono*.

Таким чином, для забезпечення ефективного доступу до правосуддя та мінімізації ризиків конвенційних порушень, національне законодавство України має бути гармонізоване з кумулятивною двокритеріальною моделлю ЄСПЛ. Лише повна імплементація фінансового критерію та критерію «інтересів правосуддя» гарантує, що конституційне право на захист буде реалізовано як практичне і дієве, а не формальне.

Література

1. Яновська О. Г. Європейські стандарти надання безоплатної правової допомоги в кримінальному судочинстві: проблеми реалізації в Україні. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 6-1(2). С. 199–202.

2. Макбрайд Д. *Європейська конвенція з прав людини та кримінальний процес*: посібник. Переклад Д. Шкрюба. Рада Європи, Ген. директорат з прав людини і прав. питань. Київ: К.І.С., 2010. 576 с.

3. Про безоплатну правничу допомогу : Закон України від 2 червня 2011 р. № 3460-VI / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/3460-17#Text> (дата звернення: 21.10.2025).

4. Про адвокатуру та адвокатську діяльність : Закон України від 5 липня 2012 р. № 5076-VI / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/5076-17#Text> (дата звернення: 21.10.2025).

DOI <https://doi.org/10.36059/978-966-397-557-3-27>

МІЖНАРОДНЕ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ЦИФРОВИХ ТЕХНОЛОГІЙ У КОНТЕКСТІ ЗАХИСТУ ПРАВ ЛЮДИНИ

Олійник А. А.

*аспірант кафедри адміністративного і кримінального права,
Дніпровський національний університет імені Олеся Гончара
м. Дніпро, Україна*

Сучасні кримінальні правопорушення у цифровій сфері за своєю природою мають транскордонний характер, оскільки вони не обмежуються лише територією однієї країни чи віртуальним простором. Ці злочини, що набувають глобального, міждержавного та міжнародного характеру,

створюють виклики для національного суверенітету та правоохоронної системи. Злочинність у цифровій сфері набула глобального масштабу, що унеможливує ефективну превенцію виключно на національному рівні. Це вимагає міжнародної координації для захисту національного суверенітету та безпеки громадян.

Основною проблемою для правоохоронних органів під час розслідування є складність ідентифікації злочинця (анонімність, використання проксі-серверів), визначення територіальної юрисдикції та застосування відповідних правових норм [1]. Цей конфлікт між віртуальною природою злочину та традиційними територіальними принципами права паралізує ефективність національних механізмів.

Таким чином, міжнародне співробітництво стає не просто бажаним, а критично необхідним імперативом для забезпечення міжнародної інформаційної безпеки. Оскільки міжнародне право лише розпочинає регулювати цю динамічну сферу, стає очевидною нагальна потреба у розробці та уніфікації міжнародно-правових засобів для ефективної превенції та захисту цифрових прав громадян.

Низка ключових міжнародних документів підкреслює, що злочинність у сфері інформаційних технологій становить екзистенційну загрозу не лише національній безпеці окремих країн, але й безпеці людства та міжнародному правопорядку. Ця глобальна турбованість знайшла своє відображення у міждержавних угодах, які формують універсальні стандарти превенції та боротьби з кіберзлочинністю.

На основі того, що злочинність у сфері ІТ є глобальною загрозою, Бангкокська декларація та Декларація ООН про злочинність і суспільну безпеку заклали політико-правову основу для стратегічних союзів та визначили необхідність комплексної, скоординованої протидії транснаціональній злочинності [2, 3]. Зокрема, Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) стала першим універсальним договором, що юридично зобов'язав держави гармонізувати своє кримінальне та процесуальне законодавство [4]. Таким чином, ці документи спільно формують базові міжнародні стандарти та практичні механізми для ефективної превенції кіберзагроз, що є критично важливим для захисту прав людини.

Резолюція 58/175 Генеральної Асамблеї ООН стала ключовим кроком у формуванні універсальних стандартів протидії кіберзлочинності, визнавши її глобальну та транснаціональну загрозу економічному розвитку, національній безпеці та міжнародній стабільності [5]. У документі підкреслено, що традиційні правові механізми недостатні для боротьби зі злочинами, де складно визначити юрисдикцію та ідентифікувати злочинця. З огляду на це, ООН закликала держави-члени до термінового посилення двостороннього та багатостороннього співробітництва, включаючи обмін

інформацією та взаємну правову допомогу. Резолюція зобов'язує країни удосконалювати національне законодавство та гармонізувати його з міжнародними інструментами, такими як Будапештська конвенція, підкреслюючи необхідність протидії неправомірному використанню ІТ (наприклад, для тероризму та шахрайства). Таким чином, Резолюція заклала політичний фундамент для проактивного запобігання кіберзлочинам, що є позитивним зобов'язанням держав щодо захисту цифрових прав своїх громадян.

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) є першим міжнародним договором, спрямованим на боротьбу з інтернет-злочинністю та комп'ютерною злочинністю (кіберзлочинністю). Конвенція була створена у відповідь на зростання кіберзлочинності наприкінці 1990-х років у зв'язку із збільшенням використання Інтернету. Станом на квітень 2023 р. Конвенцію ратифікували 68 країн (Україна її ратифікувала 07.09.2005 року; проти Конвенції виступає рф і зазвичай відмовляється співпрацювати з правоохоронними органами у розслідуванні кіберзлочинів).

Просуваючи загальні стандарти розслідування та судового переслідування кіберзлочинів Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) ставить за мету: збалансувати ефективну правоохоронну діяльність із захистом фундаментальних прав людини; установити рамки для взаємодопомоги між країнами у сфері кібербезпеки; дозволяти країнам обмінюватися інформацією, ресурсами у процесі розслідування кіберзлочинів; гармонізувати національне законодавство та посилити співпрацю у транснаціональних відносинах щодо кібербезпеки [4].

Будапештська конвенція про кіберзлочинність залишається в авангарді як основний міжнародно-правовий стандарт щодо кіберзлочинності та електронних доказів. Адже очевидно, що за умов агресії рф проти України загрози кіберзлочинності стають дедалі складнішими, тому, в умовах сьогодення, важливо, щоб вітчизняні правові системи були оснащені засобами для ефективного розслідування кіберзлочинів, одночасно забезпечуючи захист прав людини [6].

Міжнародні документи закріплюють необхідність спільного протистояння кіберзлочинам через два критично важливі механізми: вимогу до держав-членів прийняти ефективне національне законодавство, яке забезпечує взаємодопомогу у розслідуванні (міжнародне співробітництво та гармонізація); законодавство не повинно порушувати національне законодавство окремої країни та умови міжнародних угод (насамперед ЄКПЛ), стороною яких вона є (захист прав людини). Таким чином, міжнародно-правові засади створюють рамкові умови, які зобов'язують держави будувати свою національну превентивну практику з дотриманням універсальних стандартів прав людини та верховенства права.

Функціонування міжнародно-правового механізму щодо запобігання злочинності у сфері цифрових технологій відображає низку стратегічних тенденцій та актуальних викликів, що вимагають негайної уваги в контексті захисту прав людини що стосується: а) міжнародного співробітництва та глобалізації, що стає критичною умовою для протидії кіберзлочинності та забезпечення кіберстійкості національних систем; б) розвитку міжнародних правових стандартів, що сприяє встановленню чітких, єдиних правил та процедур міждержавної взаємодії. Це забезпечує верховенство права та передбачуваність у сфері цифрового захисту; в) складності, організованості та взаємопов'язаності інформаційних злочинів із транснаціональною організованою злочинністю, що вимагає спільних, скоординованих зусиль країн для превенції та ліквідації транснаціональних кіберугруповань; г) потреби у відповідності положень щодо криміналізації та процесуальних повноважень правоохоронних органів. Спрощення та уніфікація правових рамок є ключем до ефективного використання інструментів міжнародного співробітництва, що прямо впливає на захист прав людини; д) активізації розробки практичних заходів з мінімізації загроз для дітей. Зосередження уваги на захисті дітей від онлайн-насилюства, грумінгу та інших цифрових загроз є прямим втіленням принципу найкращих інтересів дитини та відображає найвищий гуманітарний стандарт міжнародного права.

У рамках міжнародного співробітництва щодо запобігання злочинності у сфері цифрових технологій, особливу увагу сьогодні привертають новітні технологічні та правові виклики, які потребують негайної уніфікації стандартів.

Сферами, що формують найактуальніші завдання для міжнародного запобігання, є: розвиток гід- та блокчейн-технологій, впровадження криптовалюти та формування банків віртуальної власності, що вимагає розробки уніфікованих правил для протидії відмиванню коштів та шахрайству; ефективне використання мережі Інтернету, соціальних мереж та комп'ютерних ігор, а також розвиток Інтернету речей та електронної комерції, що створює нові канали для шахрайства та загроз приватності; запровадження процедури біометричних паспортів (ID-карток) та створення новаторських стартапів, що ставить питання про захист персональних даних та інтелектуальної власності.

Міжнародне запобігання злочинності у сфері цифрових технологій є безумовним імперативом для сучасної держави, оскільки воно слугує основним інструментом виконання позитивних зобов'язань із захисту прав людини (включно з правом дитини) у глобалізованому кіберпросторі.

Таким чином, Міжнародне запобігання виступає як фундаментальний механізм імплементації універсальних стандартів та є ключовим індикатором готовності національної правової системи до захисту прав людини в цифрову епоху.

Література

1. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. К.: МНДЦ, 2009. № 19. С. 240–247.
2. Бангкокська декларація «Взаємодія і заходи у відповідь: стратегічні союзи в сфері попередження злочинності і кримінального правосуддя»: Прийнята на Одинадцятому Конгресі ООН з попередження злочинності і кримінального правосуддя. URL: http://www.un.org/ru/documents/decl_conv/declarations/bangkok_declaration.shtml
3. Декларація ООН Про злочинність і суспільну безпеку. https://zakon.rada.gov.ua/laws/show/995_371#Text
4. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
5. Широкова-Мурараш О. Г., Акчурін Ю. Р. Міжнародно-правові заходи щодо упередження злочинності у сфері інформаційної безпеки. *Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм*. 2010. Вип. 2. С. 78-82.
6. Будапештська конвенція про кіберзлочинність як основний міжнародно – правовий стандарт щодо кіберзлочинності. URL: <https://law.chnu.edu.ua/budapeshtska-konventsia-pro-kiberzlochynnist/>

Дослідження частково профінансовано Міністерством закордонних справ Чеської Республіки в межах проєкту 25-PKV-UM-004 «Development of Education, Research, and International Cooperation at Oles Honchar Dnipro National University (DNU)», реалізованого Карловим університетом і Дніпровським національним університетом імені Олеся Гончара.