

foreign affairs. It is argued that while criteria form the basis for dividing special missions into types, the specific type does not dictate their legal status; rather, the status depends on the functions (tasks) entrusted to them. Furthermore, it is proven that special missions are less formalized bodies in the sphere of external relations, yet they are capable of resolving highly complex tasks of interstate importance much faster and more professionally than permanent diplomatic missions.

The author identifies conceptual approaches to the typification of missions, allowing for their differentiation by political weight, duration, and the legal status of participants. The research results contribute to a deeper understanding of flexible foreign policy instruments and can be used to improve the protocol support for international visits.

Keywords: diplomatic law, high-level missions, political and technical missions, special missions, paradiplomatic missions, ceremonial missions, ad hoc missions.

*Дата першого надходження статті до видання: 13.04.2026 р.
Дата прийняття статті до друку після рецензування: 22.04.2026 р.*

УДК 341:004.9

DOI 10.31558/2786-5835.2026.1.1.8

Іванов Андрій Валерійович,

кандидат юридичних наук,

доцент кафедри фундаментальних і галузевих юридичних наук

Кременчуцького національного університету імені Михайла Остроградського

ORCID: <https://orcid.org/0000-0002-5934-6837>

Григор'єв Сергій Сергійович,

здобувач першого (бакалаврського) рівня вищої освіти

факультету права, гуманітарних та соціальних наук

Кременчуцького національного університету імені Михайла Остроградського

ЕВОЛЮЦІЯ МІЖНАРОДНОГО ПРАВА В УМОВАХ ЦИФРОВІЗАЦІЇ

Стаття присвячена аналізу впливу цифровізації на сучасне міжнародне право, міжнародні відносини та захист прав людини. Автор наголошує, що кіберпростір сьогодні є невід'ємним складником міжнародних відносин. Він відкриває нові горизонти для співпраці між державними та недержавними суб'єктами, сприяє зближенню людей різних країн, але водночас створює серйозні виклики для глобальної стабільності та безпеки.

Розглядаються дуалістичні наслідки оцифрування. Позитивний аспект полягає в полегшенні доступу до правової інформації, спрощенні її поширення та розширенні змісту традиційних прав, зокрема свободи вираження поглядів (ст. 19 Загальної декларації прав людини 1948 р. та ст. 10 Конвенції про захист прав людини 1950 р.). Як приклад автоматизації державних послуг наводиться український портал «Дія». Негативний бік пов'язаний з ризиками порушення права на приватне життя через обробку персональних даних, несанкціоноване використання інформації, а також появою нових загроз.

Особливу увагу приділено новим викликам: кібератакам, інформаційним війнам, застосуванню штучного інтелекту у військовій сфері та стрімкому поширенню кіберзлочинності. Автор зазначає, що міжнародне гуманітарне право та наявні механізми захисту прав людини ще недостатньо адаптовані до цих реалій. Появляються нові категорії прав, як-от право на захист від кібервійни та право на мир у цифровому просторі.

Аналізується проблема практичної реалізації цифрових прав. Незважаючи на їх закріплення в національному законодавстві (зокрема в ЄС), судові та правоохоронні органи стика-

ються з труднощами кваліфікації правопорушень через анонімність, швидкість процесів і брак відповідних інструментів у національних системах.

У висновку підкреслюється необхідність адаптації міжнародного права: посилення міжнародного співробітництва, розробки нових конвенцій щодо регулювання ІІІ та кібербезпеки, створення ефективних механізмів відповідальності (включаючи для організованих кіберугруповань) та збереження балансу між інноваційним розвитком і захистом прав людини. Ключовим завданням сучасності є формування глобальних етичних стандартів у цифровій сфері.

Ключові слова: міжнародне право, цифровізація, кіберзлочинність, права людини, кібербезпека.

Постановка проблеми. Кіберпростір наразі є невід’ємною частиною міжнародних відносин. Безліч технологій може зблизити людей з різних країн та відкрити нові горизонти, створюючи в такий спосіб нові можливості для співпраці між державними та недержавними суб’єктами. Держави залежать від функціонування інфраструктур, що сприяє виникненню нових викликів. Операції в цифровому просторі, що здійснюються державними та недержавними суб’єктами, можуть поставити під загрозу міжнародну стабільність.

Аналіз останніх досліджень і публікацій. Тема еволюції міжнародного права в умовах цифровізації є однією з найбільш динамічних у сучасній юридичній науці. У 2023–2026 роках вийшло значне число монографій, статей та звітів міжнародних організацій, які підкреслюють трансформаційний вплив цифрових технологій (ІІІ, кіберпростір, великі дані) на міжнародне право, права людини та міжнародну безпеку.

Українські науковці активно розвивають цю тематику. Наприклад, І. В. Захарчук у статті «Міжнародне право в умовах цифровізації: становлення четвертого покоління прав людини» (2025) аналізує еволюцію концепції поколінь прав людини та виділяє нові цифрові права (право на доступ до інтернету, захист персональних даних, цифрову безпеку, інформаційну автономію та справедливе використання ІІІ). Автор наголошує на міждисциплінарному характері цих прав і ролі міжнародних організацій (ООН, Рада Європи, ЄС, ЮНЕСКО) у їх формуванні. А. Р. Лабик розглядає вплив цифровізації на міжнародне право прав людини, підкреслюючи появу нових прав і переосмислення традиційних.

Зарубіжні дослідження 2024–2025 років акцентують на гнучкій еволюційній архітектурі міжнародного кіберправа. К. Balarabe (2025) закликає до адаптивної нормативної бази, яка встигатиме за технологічними змінами, зокрема в питаннях суверенітету, атрибуції та кібервійни.

У сфері кібербезпеки та кіберзлочинності ключовим є розвиток **Будапештської конвенції про кіберзлочинність**. Другий додатковий протокол (2022, підписаний багатьма країнами) посилює співпрацю щодо отримання електронних доказів з урахуванням захисту прав людини.

Отже, сучасна наукова література одностайно констатує, що цифровізація радикально трансформує міжнародне право, вимагаючи як актуалізації наявних норм, так і створення нових інструментів.

Постановка завдання. Стаття присвячена дослідженню впливу процесів цифровізації на сучасне міжнародне право, систему міжнародних відносин та механізми захисту прав людини.

Виклад основного матеріалу. Міжнародне право має центральне значення у вирішенні питань можливостей та ризиків, пов'язаних із використанням інформаційних технологій у міжнародному контексті.

Безперечно, говорити про масштабні зміни для міжнародного права прав людини на етапі оцифрування зарано. Водночас цілковите заперечення його впливу на відповідну сферу також було б недоцільним. З одного боку, оцифрування сприяє полегшенню доступу до необхідної, зокрема і правової, інформації, а також спрощує її поширення. Отже, обов'язок держав щодо забезпечення свободи вираження поглядів, передбаченої ст. 19 Загальної декларації прав людини 1948 р., ст. 10 Конвенції про захист прав людини та основоположних свобод 1950 р., наповнюється новим змістом [1, с. 321]. Це закладає основи для розширення правової природи традиційних прав людини. З іншого боку, перетворення персональних даних особи у цифровий формат спричиняє виникнення ризиків щодо її несанкціонованого використання, що веде до порушення права на приватне життя людини, гарантоване міжнародними актами універсального та регіонального рівнів [2 с. 431].

Глибокі перетворення соціально-економічного характеру зумовлюють зміни також у сфері забезпечення та захисту прав людини, адже саме цифрова трансформація дала змогу дізнатися про штучний інтелект, машинне навчання, автоматизовані системи озброєння. На шальках терезів опинилися, з одного боку, можливість автоматизації різноманітних послуг, зокрема і державних (наприклад, через вебпортал «Дія» в Україні), обробки та аналізу даних, виконання команд без участі людини, зменшення людських втрат у збройних конфліктах тощо, а з іншого, – непередбачуваність таких цифрових екосистем, відсутність аргументації щодо прийнятих рішень, існування численних шкідливих програм та застосунків, виявити і запобігти яким стає все складніше. Усе це вимагає встановлення механізмів, які б дали змогу не допускати порушення прав людини, а в разі їх допущення – забезпечувати ефективний захист і справедливу сатисфакцію для кожного. Водночас держави та міжнародна спільнота загалом стоять перед необхідністю зберігати належний баланс між надмірною зарегульованістю цифрової сфери та повною відсутністю втручання у кіберпростір [2, с. 432].

Цифровізація призводить до появи нових загроз у сфері міжнародної безпеки: кібератак, інформаційних війн, застосування штучного інтелекту у військовій

сфері. Це створює виклик для міжнародного права, адже з'являються нові категорії прав: право на захист від кібервійни, право на мир у цифровому вимірі. Водночас міжнародне гуманітарне право поки що не адаптоване до таких реалій [3, с. 357].

Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності – характерного наслідку глобалізації інформаційних процесів [4, с. 333]. М. І. Саєнко зазначає, що кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер. Характерні ознаки кіберзлочинності приваблюють людство, що означає збільшення кількості осіб, які чинять протиправну діяльність. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже, використовувати ці методи може будь-хто – від дрібних злодіїв до досвідчених.

Міжнародне право має передбачити створення механізмів правового захисту громадян, які стали жертвами таких злочинів, зокрема через обов'язкову імплементацію державами-членами міжнародних стандартів кібербезпеки. Також особливої уваги заслуговує визначення кіберзлочинності як явища, що охоплює як індивідуальні, так і організовані форми злочинної діяльності. У цьому контексті особливого значення набуває розробка механізмів притягнення до відповідальності не лише індивідів, але й організованих угруповань, які використовують кіберпростір для досягнення своїх злочинних цілей [4, с. 334].

Попри те, що багато країн уже проголосили цифрові права на рівні законів, реальне їх дотримання часто лишається лише на папері. Судді та слідчі відчують брак чітких критеріїв для оцінки порушень в онлайн-середовищі, а застарілі національні процедури погано пристосовані до швидкості та анонімності кіберпростору.

Водночас міжнародні судові інституції, зокрема Європейський суд з прав людини, поступово формують практику, що розширює традиційні права у цифровому вимірі. Наприклад, право на приватність застосовується до захисту персональних даних у мережі.

На рівні ООН запроваджено такі ініціативи:

Global Digital Compact (Глобальний цифровий пакт, 2024) – прийнятий на Саміті майбутнього (Summit of the Future) у вересні 2024 року як частина Pact for the Future. Встановлює принципи глобального цифрового співробітництва, управління ІІІ, закриття цифрового розриву, захист прав людини в цифровому середовищі та безпечний інтернет. Передбачає створення International Scientific Panel on AI та Global Dialogue on AI Governance.

Open-Ended Working Group (OEWG) on ICT Security (2021–2025) та новий Global Mechanism (з 2026) – постійний механізм ООН з питань безпеки у вико-

ристанні інформаційно-комунікаційних технологій (ІКТ). Обговорює норми відповідальної поведінки держав у кіберпросторі, застосування міжнародного права (включаючи гуманітарне право) до кібероперацій, заходи зміцнення довіри та capacity-building. У 2025 році OEWG завершив роботу та передав естафету постійному Global Mechanism (розпочав роботу у березні 2026).

Конвенція ООН проти кіберзлочинності (United Nations Convention against Cybercrime, Hanoi Convention) – прийнята Генеральною Асамблеєю у грудні 2024 року. Відкрита для підписання з жовтня 2025 року. Є першим глобальним договором з кримінального правосуддя за понад 20 років, метою якого є посилення міжнародної співпраці, обмін електронними доказами, боротьба з кіберзлочинністю (включаючи транснаціональні злочини).

High-Level Advisory Body on Artificial Intelligence ООН – рекомендації щодо глобального управління ШІ.

Висновки. Цифровізація суттєво трансформує міжнародне право, створюючи як нові можливості для реалізації прав людини, так і серйозні виклики у сфері безпеки та приватності. Вона сприяє розширенню змісту традиційних прав, водночас породжуючи нові. Зростання кіберзагроз, розвиток штучного інтелекту та кіберзлочинності вимагають адаптації міжнародно-правових норм і посилення співпраці між державами. Отже, ключовим завданням сучасного міжнародного права є забезпечення балансу між розвитком цифрових технологій і ефективним захистом прав людини.

Для досягнення цього балансу необхідна системна робота на кількох рівнях. По-перше, актуалізація наявних міжнародних договорів та розробка нових спеціалізованих конвенцій, присвячених регулюванню штучного інтелекту, захисту даних і протидії кіберзагрозам. По-друге, створення ефективних платформ для обміну інформацією та оперативного реагування між державами, як-от INTERPOL, Europol та регіональні кіберцентри. По-третє, важливим є залучення недержавних акторів – технологічних компаній, громадських організацій та експертів – до процесу нормотворення, оскільки саме вони часто володіють найсучаснішими технологічними знаннями.

До того ж перспективним напрямом є формування глобальних стандартів етичного використання цифрових технологій, зокрема у сфері штучного інтелекту. Це дасть змогу не лише реагувати на вже наявні загрози, але й передбачати майбутні ризики, пов'язані з розвитком автономних систем та квантових обчислень. У кінцевому підсумку успіх цифрової трансформації міжнародного права залежатиме від здатності світової спільноти поєднати інноваційний розвиток із непорушністю основоположних прав і свобод людини.

Список використаних джерел

1. Юрченко М. М., Костова Н. І. Міжнародні стандарти ЄС щодо доступу до публічної інформації: порівняльний аналіз з Україною. *Юридичний науковий електронний журнал*. 2021. № 5. С. 320–322. DOI: <https://doi.org/10.32782/2524-0374/2021-5/75>
2. Лабик А. Р. Міжнародне право прав людини в умовах цифровізації: аналіз ключових понять. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 6. С. 429–433. DOI: <https://doi.org/10.24144/2788-6018.2025.06.3.65>
3. Захарчук І. В. Міжнародне право в умовах цифровізації: становлення четвертого покоління прав людини. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 5. С. 353–359. DOI: <https://doi.org/10.24144/2788-6018.2025.05.3.52>
4. Вареник О. С. Міжнародно-правове регулювання кіберзлочинності в умовах глобалізації. *Науковий вісник публічного та приватного права*. 2024. № 4 С. 331–337. DOI: <https://doi.org/10.32844/2618-1258.2024.4.55>
5. Сасенко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. Вип. 64. С. 386–391. DOI: <https://doi.org/10.32844/2618-1258.2024.4.55>

Andrii Ivanov, Serhii Hryhoriev. The Evolution of International Law in the Context of Digitalization

The article is dedicated to analyzing the impact of digitalization on modern international law, international relations, and the protection of human rights. The author emphasizes that cyberspace today constitutes an integral part of international relations. It opens new horizons for cooperation between state and non-state actors, facilitates the rapprochement of people from different countries, but at the same time creates serious challenges to global stability and security.

The dualistic consequences of digitization are examined. The positive aspect lies in facilitating access to legal information, simplifying its dissemination, and expanding the scope of traditional rights, particularly freedom of expression (Article 19 of the Universal Declaration of Human Rights of 1948 and Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950). The Ukrainian portal “Diia” is cited as an example of the automation of public services.

The negative side is associated with risks of violating the right to privacy through the processing of personal data, unauthorized use of information, and the emergence of new threats. Particular attention is paid to new challenges: cyberattacks, information warfare, the use of artificial intelligence in the military sphere, and the rapid spread of cybercrime.

The author notes that international humanitarian law and existing human rights protection mechanisms are not yet sufficiently adapted to these realities. New categories of rights are emerging, such as the right to protection from cyber warfare and the right to peace in the digital space. The article analyzes the problem of the practical implementation of digital rights. Despite their enshrinement in national legislation (particularly in the EU), judicial and law enforcement authorities face difficulties in qualifying offenses due to anonymity, the high speed of processes, and the lack of appropriate tools in national legal systems.

In conclusion, the necessity of adapting international law is underlined: strengthening international cooperation, developing new conventions on the regulation of AI and cybersecurity, creating effective accountability mechanisms (including for organized cyber groups), and maintaining a balance between innovative development and the protection of human rights. The key task of our time is the formation of global ethical standards in the digital sphere.

Keywords: *international law, digitalization, cybercrime, human rights, cybersecurity.*

*Дата першого надходження статті до видання: 12.04.2026 р.
Дата прийняття статті до друку після рецензування: 20.04.2026 р.*