

INTERNATIONAL SCIENCE SPACE

*New horizons of science: interdisciplinary research in
a changing world*

International scientific and practical conference



*27.10.2026 – Uzhhorod, Ukraine – Prague, Czech Republic
collection of scientific papers*

УДК 001.89:34:37:159.9:61

DOI -

The 7th International scientific and practical conference «New horizons of science: interdisciplinary research in a changing world» (October 27, 2026, Uzhhorod-Prague) ISS “ <https://iscience-space.com/>”: Uzhhorod, Ukraine – Prague, Czech Republic, 2026. 192 p.

7-ма міжнародна науково-практична конференція «New horizons of science: interdisciplinary research in a changing world» (27 жовтня, 2026 р., Ужгород-Прага). ISS “<https://iscience-space.com/>”: Ужгород, Україна-Прага, Чеська Республіка, 2026. 192 с.

The recommended citation for this publication is/ Рекомендоване бібліографічне посилання на це видання:

Kashuba V. Theoretical foundations of developing technological competencies in lower secondary school students. Proceedings of the 7th International scientific and practical conference «New horizons of science: interdisciplinary research in a changing world» (October 27, 2026, Uzhhorod-Prague) International science space: Uzhhorod, Ukraine – Prague, Czech Republic, 2026. Pp. 167-173.

The materials of the conference are publicly available under the terms of the CC BY NC 4.0 International license.

EDITORIAL BOARD:

Veronika Berch – Doctor of Law, Associate Professor, Professor of the Department of Constitutional Law and Comparative Jurisprudence, Uzhhorod National University, Founder.

Viktoriia Prodan – PhD in Law, Senior Lecturer at the Department of Constitutional Law and Comparative Jurisprudence, Uzhhorod National University, Founder.

Yurii Bysaha – Doctor of Law, Professor, Honored Lawyer of Ukraine, Head of the Department of Constitutional Law and Comparative Jurisprudence, Uzhhorod National University.

Larysa Zhdankina – PhD in Law, Researcher in Private Law, University of Glasgow / Scottish Parliament.

Elżbieta Żywucka-Kozłowska – Professor, Doctor of Law, Criminologist, Expert in Forensic Identification, University of Warmia and Mazury.

Vasyl Moskov – PhD in Pedagogy, Executive Director of the Academy of Science and Technology (Prague, Czech Republic), International Educational Manager, Interdisciplinary Researcher in Educational Policy, Digital Transformation, Artificial Intelligence and Law in the Digital Society.

Massimiliano Blasone – Attorney at the Supreme Court of Italy, International Expert in Civil Procedure and Judicial Enforcement.

Damian Wąsik – PhD in Law, Wyższa Szkoła Kształcenia Zawodowego, Interdisciplinary Legal Researcher in Criminal, Medical and Administrative Law, Specialist in Electoral Crimes and Healthcare Law.

Natalia Wąsik – PhD in Law, Wyższa Szkoła Kształcenia Zawodowego, Legal Researcher in Medical Law and Healthcare Liability, Specialist in Patients' Rights and Medical Errors.

This collection of materials from an international scientific and practical conference addresses pressing issues regarding the development of law, the state, and society amidst contemporary socio-political and technological transformations. The primary focus is on constitutionalism, judicial independence, constitutional identity, and the protection of human rights and freedoms within the context of martial law and European integration. The publication covers legal aspects of the digital transformation of public authority, the safeguarding of digital rights, personal data protection, cybersecurity, and digital sovereignty. It also examines the challenges of legally regulating artificial intelligence, its impact on electoral processes, and mechanisms for legal liability. The interdisciplinary nature of the volume is further enriched by research in pedagogy, psychology, and medicine—specifically concerning the development of technological competencies, the influence of the social environment on the individual, and modern approaches to medical diagnostics. The materials presented facilitate a comprehensive understanding of current scientific issues and outline prospects for future research.

Збірник матеріалів міжнародної науково-практичної конференції присвячено актуальним проблемам розвитку права, держави та суспільства в умовах сучасних соціально-політичних і технологічних трансформацій. Основну увагу зосереджено на питаннях конституціоналізму, незалежності судової влади, конституційної ідентичності, захисту прав і свобод людини в умовах воєнного стану та європейської інтеграції. Висвітлено правові аспекти цифрової трансформації публічної влади, забезпечення цифрових прав, захисту персональних даних, кібербезпеки та цифрового суверенітету. Окремо розглянуто виклики правового регулювання штучного інтелекту, його вплив на виборчий процес і механізми юридичної відповідальності. Міждисциплінарний характер видання доповнюють дослідження у сфері педагогіки, психології та медицини, присвячені розвитку технологічних компетентностей, впливу соціального середовища на особистість і сучасним підходам до медичної діагностики. Представлені матеріали сприяють комплексному осмисленню актуальних наукових проблем і визначенню перспектив їх подальшого дослідження.

e-mail: isciencespace@gmail.com

homepage: <https://iscience-space.com/>

© International Educational Platform «International Science Space»

©2026 Authors of the articles

ЗМІСТ

Секція 1. Юридичні науки та державне управління

- Бабей А.А.** Конституційні гарантії незалежності судової влади в умовах інституційних реформ **9-16**
- Біров Н.Е.** Конституційна ідентичність України в контексті європейської інтеграції **17-27**
- Гелетій М.В.** Система правових стандартів захисту прав людини в умовах воєнного стану **28-30**
- Готра В.В.** Конституційні межі обмеження прав і свобод людини в умовах воєнного стану **31-38**
- Грига Н.В.** Конституційно-правовий статус суду присяжних як форми участі народу у здійсненні судової влади **39-44**
- Гудим В.Л.** Національна та конституційна ідентичність: теоретичні засади детермінації **45-48**
- Дарвай В.І.** Конституційно-правові гарантії захисту персональних даних в умовах цифрової держави **49-58**
- Зейкан В.В.** Конституційно-правові засади цифрової трансформації публічної влади в Україні **59-66**
- Лендшел А.В.** Цифрові права людини у системі сучасного конституціоналізму **67-74**
- Луканич Я.І.** Свобода вираження поглядів у соціальних мережах: співвідношення приватної модерації та конституційних гарантій **75-78**

Марковцій К. Цифровий суверенітет держави як категорія сучасного конституційного права **79-92**

Музичук М. Правові механізми захисту прав осіб з інвалідністю в сучасних державно-політичних умовах **93-96**

Рішко Є.П. Електронне голосування на виборах: конституційні гарантії, ризики та межі цифровізації виборчого процесу **97-114**

Самойленко Ю.В. Право на доступ до інтернету як новітнє конституційне право людини: доктринальні та нормативні підходи **115-123**

Степанова А.М. Біометричні дані як об'єкт конституційно-правової охорони **124-127**

Торчинович Н.П. Кібербезпека як елемент конституційної безпеки держави **128-138**

Ухаль К.П. Цивільно-правова відповідальність за шкоду, завдану системами штучного інтелекту: підходи Європейського Союзу та перспективи вдосконалення законодавства **139-148**

Фединець М.М. Конституційні межі використання штучного інтелекту органами публічної влади **149-154**

Щерба О.С. Вплив автоматизованих систем штучного інтелекту на виборчий процес **155-166**

Секція 14. Педагогічні науки

Кашуба В.В. Theoretical foundations of developing technological competencies in lower secondary school students **167-173**

Секція 15. Психологічні науки

Ничипорук Я.О. Вплив соціальних мереж на формування соціальної ідентичності та самооцінки сучасної молоді **174-180**

Федоренко В.В. Вплив групового тиску на прийняття особистих рішень **181-187**

Секція 16. Медичні науки

Бевзюк А.Є. Комплексна діагностика спадкового холестазу у дітей **188-191**

СЕКЦІЯ 1. ЮРИДИЧНІ НАУКИ ТА ДЕРЖАВНЕ УПРАВЛІННЯ

УДК 342.56:342.4(477)

КОНСТИТУЦІЙНІ ГАРАНТІЇ НЕЗАЛЕЖНОСТІ СУДОВОЇ ВЛАДИ В УМОВАХ ІНСТИТУЦІЙНИХ РЕФОРМ

Бабей Андрій Андрійович,
здобувач другого (магістерського) рівня вищої освіти,
ФПП, 2 група, Ужгородський університет,
м. Ужгород, Україна

Реформування органів суддівського врядування майже не припиняється в Україні з часу конституційних змін 2016 року. Щоразу воно змушує законодавця шукати рівновагу між потребою очистити судову систему від недоброчесності та обов'язком зберегти конституційні запобіжники проти політичного тиску, тому центральне питання дослідження полягає в тому, де закінчується легітимне оновлення інституцій і починається втручання, здатне підірвати самостійність судової гілки. Гостроти цьому питанню надає спостереження науковців, що стабільність судової влади помітно залежить від зміни політичної еліти. Наочний приклад дала осінь 2019 року: Закон № 193-IX припинив повноваження чинного складу Вищої кваліфікаційної комісії суддів і зупинив діяльність органу, який відіграє ключову роль у кадровому забезпеченні судів [1; 2].

Конституційну основу цієї засади становить насамперед стаття 126, за якою незалежність і недоторканність судді гарантуються Конституцією та законами, вплив на суддю у будь-який спосіб заборонено, а посаду суддя обіймає безстроково [3, ст. 126]. До неї приєднується стаття 129, згідно з якою суддя, здійснюючи правосуддя, є незалежним і керується верховенством права

[3, ст. 129]. Інституційний вимір забезпечила реформа 2016 року, що замінила Вищу раду юстиції Вищою радою правосуддя з ширшими повноваженнями щодо звільнення, переведення та затримання суддів [4]. Наукова думка розвиває цей підхід. Н. Гданський розглядає інституційну автономію як результат дії не лише статей 126 і 129, а й статей 6, 8, 128, 129-1, 130, 130-1 та 131, і водночас констатує ознаки кризи у відносинах законодавчої та судової гілок [5, с. 283–284]. С. Пушкар, у свою чергу, пропонує розуміти гарантії як систему заходів і механізмів, що унеможливають неправомірне втручання, вплив або тиск на суддю, і підкреслює ключову роль Вищої ради правосуддя та тенденцію до зменшення кількості випадків втручання впродовж 2020–2022 років [6].

Міжнародні стандарти доповнюють національний контур. Рекомендація СМ/Рес(2010)12 Комітету Міністрів Ради Європи трактує таку самостійність як гарантію поваги до прав людини, а не привілей суддів [7]. Практика Європейського суду з прав людини показує, що порушення виникають передусім у процедурах відповідальності та усунення від посади. У справі «Олександр Волков проти України» Суд одностайно встановив чотири порушення статті 6 та порушення статті 8 Конвенції, а відсутність безсторонності Вищої ради юстиції і парламентського комітету стала підставою для вимоги поновити заявника на посаді [8]. У справі «Гженда проти Польщі» Велика палата більшістю у шістнадцять голосів проти одного визнала порушення пункту 1 статті 6 через відсутність судового оскарження дострокового припинення мандата судді в Національній раді судівництва [9]. Право Європейського Союзу рухається в тому самому напрямі: Суд ЄС у справі С-64/16 пов'язав судову самостійність зі статтею 19(1) Договору про ЄС, хоч і визнав, що загальні скорочення винагороди в межах бюджетної консолідації їй не суперечать [10].

Національна практика останніх років ілюструє напругу між реформою та гарантіями. Конституційний Суд у Рішенні № 4-р/2020 визнав неконституційною норму про утворення Комісії з питань доброчесності та етики, повноваження якої охоплювали оцінку членів Вищої ради правосуддя та суддів Верховного Суду [11]. Рада Європи у своєму висновку зазначила, що парламентська більшість і уряд не повинні ставити під сумнів призначення чи перебування на посаді суддів, призначених належним чином [12].

Закон № 1635-IX [13], який ураховував рекомендації Венеційської комісії, викладені в терміновому спільному висновку від 5 липня 2021 року [14], створив Етичну раду, де за розподілу голосів три проти трьох переважає позиція міжнародних експертів. Верховний Суд у конституційному поданні застеріг, що така конструкція, як і повторне оцінювання членів Вищої ради правосуддя та припинення їхніх повноважень законом, порушує принцип безперервності органу і вимоги статті 126 [15]. Венеційська комісія, навпаки, згодом оцінила роботу Етичної ради як успішну і запропонувала використати її досвід для інших органів [16]. Європейська комісія у Звіті 2025 року відзначила, що самостійність і неупередженість суддів гарантовані конституцією та законодавством, проте вади в законі й на практиці зберігаються, а довіра суспільства залишається дуже низькою [17].

Аналіз наведених джерел дає підстави сформулювати авторський висновок так: критерієм конституційності судової реформи є не суб'єкт, що її ініціює, і не декларована мета, а наявність судового контролю над кожним індивідуальним наслідком реформи для конкретного судді. Це формулювання впливає з порівняння двох ризиків, які на перший погляд протилежні, але однаково руйнують гарантію незалежності. З одного боку, справа Волкова доводить: коли рішення про звільнення ухвалює орган без ознак безсторонності

й без ефективного судового перегляду, дисциплінарна відповідальність перетворюється на інструмент тиску. З іншого боку, вимога безперервності Вищої ради правосуддя не може бути принесена в жертву швидкості очищення, бо орган, який парламент здатен розпустити звичайним законом, перестає бути гарантією і перетворюється на залежну від політичної більшості структуру.

Із цього зіставлення випливає другий складник авторської позиції: залучення закордонних фахівців узгоджується з Основним Законом лише тоді, коли водночас дотримано трьох вимог – обмеженість у часі повноважень, чітко окреслений перелік завдань і можливість оскаржити до суду вплив рішення на конкретну особу. Такий підхід відповідає логіці вердикту у справі «Гженда проти Польщі», де порушення зафіксовано не через сам факт існування наглядового органу, а через брак судового механізму для заперечення його висновку. Точка зору Верховного Суду щодо вирішального голосу фахівців в Етичній раді є обґрунтованою як запобіжник проти недотримання статті 126, проте вона не усуває потреби в зовнішньому контролі в ситуаціях, коли, на думку Європейської комісії, рівень суспільної довіри до судової системи залишається надто низьким.

Конституційність судової реформи слід перевіряти не за декларацією намірів законодавця, а за трискладовим тестом – чи зберігається безперервність органів суддівського врядування, чи обмежена участь зовнішніх акторів у часі та функціях, чи має суддя право на судовий перегляд рішення, що зачіпає його статус. Реформа, яка не проходить хоча б один із цих трьох елементів тесту, суперечить статті 126 Конституції незалежно від щирості декларованої мети.

Підсумовуючи, конституційні гарантії самостійності судової влади в Україні достатні за змістом, проте вразливі до змін політичної кон'юнктури, а найбільше страждає не сам текст Основного Закону, а стабільність органів, які

його реалізують. Для усунення цієї вразливості доцільно, по-перше, закріпити в законодавстві заборону припиняти повноваження складу Вищої ради правосуддя та Вищої кваліфікаційної комісії суддів одномоментно законом, а тимчасові процедури оновлення передбачати лише за наявності окремої конституційної підстави. По-друге, участь міжнародних експертів слід унормувати як обмежений у часі механізм із чіткими критеріями оцінювання та правом на судове оскарження рішень, що зачіпають статус судді. По-третє, з огляду на те, що Вища рада правосуддя працює у складі, меншому за повний, а за оцінкою Європейської комісії, наповнення вакансій потребує невідкладного прискорення, доцільно встановити для квот, які формуються суддівським і адвокатським з'їздами, граничні строки конкурсних процедур. По-четверте, законопроекти у сфері судоустрою мають проходити попередню експертизу Венеційської комісії ще до другого читання, а не після ухвалення, що зменшить ризик подальшого конституційного оскарження та відповідає практиці, яка вже склалася у відносинах з Радою Європи.

Список використаних джерел

1. Про внесення змін до Закону України «Про судоустрій і статус суддів» та деяких законів України щодо діяльності органів суддівського врядування : Закон України від 16 жовтня 2019 р. № 193-IX. URL: <https://zakon.rada.gov.ua/laws/show/193-20> (дата звернення: 14.10.2026).
2. Хотинська-Нор О. 3. Актуальні питання правового регулювання статусу Вищої кваліфікаційної комісії суддів України. *Вісник кримінального судочинства*. 2020. № 1–2. С. 146–154. URL: https://vkslaw.knu.ua/images/verstka/1_2020_KHOTYNSKA-NOR.pdf (дата звернення: 23.09.2026).

3. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141 (із наступними змінами). URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 23.09.2026).
4. Про Вищу раду правосуддя : Закон України від 21 грудня 2016 р. № 1798-VIII (із наступними змінами). URL: <https://zakon.rada.gov.ua/laws/show/1798-19> (дата звернення: 23.09.2026).
5. Гданський Н. Заходи щодо забезпечення інституційної незалежності судової влади. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2023. № 4 (40). С. 283–293. URL: <https://ena.lpnu.ua/items/900ee583-945d-48ca-89d7-4db9c81f5406> (дата звернення: 23.09.2026).
6. Пушкар С. І. Забезпечення незалежності суддів як гарантія їх діяльності. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2023. Вип. 78. Т. 2. С. 336–341. URL: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/56475> (дата звернення: 23.09.2026).
7. Recommendation CM/Rec(2010)12 of the Committee of Ministers to member states on judges: independence, efficiency and responsibilities : adopted by the Committee of Ministers on 17 November 2010. Strasbourg : Council of Europe, 2010. URL: <https://rm.coe.int/cmrec-2010-12-on-independence-efficiency-responsibilites-of-judges/16809f007d> (дата звернення: 23.09.2026).
8. Case of Oleksandr Volkov v. Ukraine : judgment of the European Court of Human Rights of 9 January 2013, application no. 21722/11. URL: <https://hudoc.echr.coe.int/eng?i=001-115871> (дата звернення: 23.09.2026).

9. Case of Grzęda v. Poland : judgment of the European Court of Human Rights (Grand Chamber) of 15 March 2022, application no. 43572/18. URL: <https://hudoc.echr.coe.int/eng?i=001-216400> (дата звернення: 23.09.2026).
10. Judgment of the Court (Grand Chamber) of 27 February 2018, Associação Sindical dos Juizes Portugueses v Tribunal de Contas, Case C-64/16, ECLI:EU:C:2018:117. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0064> (дата звернення: 23.09.2026).
11. Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду щодо відповідності Конституції України (конституційності) окремих положень законів України «Про судоустрій і статус суддів», «Про внесення змін до Закону України „Про судоустрій і статус суддів“ та деяких законів України щодо діяльності органів суддівського врядування», «Про Вищу раду правосуддя» від 11 березня 2020 р. № 4-р/2020. URL: <https://zakon.rada.gov.ua/laws/show/v004p710-20> (дата звернення: 24.09.2026).
12. Парламентська більшість та уряд не повинні ставити під сумнів призначення чи перебування на посаді суддів, які були призначені належним чином : висновок Ради Європи стосовно рішень Конституційного Суду України щодо судової влади. *Судова влада України*. 2020. 29 квіт. URL: <https://court.gov.ua/press/news/932438/> (дата звернення: 24.09.2026).
13. Про внесення змін до деяких законодавчих актів України щодо порядку обрання (призначення) на посади членів Вищої ради правосуддя та діяльності дисциплінарних інспекторів Вищої ради правосуддя : Закон України від 14 липня 2021 р. № 1635-IX. URL: <https://zakon.rada.gov.ua/laws/show/1635-20> (дата звернення: 24.09.2026).

14. Ukraine – Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the Draft Law on Amendments to Certain Legislative Acts Concerning the Procedure for Electing (Appointing) Members of the High Council of Justice (HCJ) and the Activities of Disciplinary Inspectors of the HCJ (Draft Law No. 5068): opinion No. 1029/2021, CDL-AD(2021)018, issued under the urgent opinion procedure. Strasbourg, 5 July 2021. URL: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2021\)018-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2021)018-e) (дата звернення: 24.09.2026).
15. Конституційне подання Верховного Суду щодо Закону України № 1635-IX: новина. Судова влада України. URL: <https://court.gov.ua/press/news/1258909/> (дата звернення: 24.09.2026).
16. The Venice Commission has again positively evaluated work of the Ethics Council: новина. Judiciary of Ukraine. 2022. URL: <https://court.gov.ua/eng/ec/pres-centr/news/1351416/> (дата звернення: 24.09.2026).
17. European Commission. Commission Staff Working Document: Ukraine 2025 Report. Brussels, 4 November 2025. SWD(2025) 759 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52025SC0759> (дата звернення: 24.09.2026).

Дата першого надходження рукопису до видання: 19.10.2026

Дата прийняття до друку рукопису після рецензування: 22.10.2026

Дата публікації: 27.10.2026

УДК 342.41+341.17:342.4(477)

КОНСТИТУЦІЙНА ІДЕНТИЧНІСТЬ УКРАЇНИ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Біров Неля Елемирівна,
студентка ОС «Магістр» юридичного факультету,
Ужгородський університет,
м. Ужгород, Україна

Надання Україні статусу кандидата на членство в Європейському Союзі та рішення Європейської ради про початок переговорів [3; 4] перевели євроінтеграцію з площини політичного курсу в площину конституційно-правових наслідків. Вступ до ЄС означає не лише імплементацію *acquis*, а й прийняття примату права Союзу та спільних цінностей, закріплених у ст. 2 Договору про ЄС (ДЄС) [5]. Водночас Союз зобов'язується поважати національні ідентичності держав-членів, притаманні їхнім основоположним політичним і конституційним структурам (ч. 2 ст. 4 ДЄС) [5]. Для України звідси випливає три питання: що саме становить її конституційну ідентичність; чи є вона обмеженням, чи ресурсом євроінтеграції; яким правовим шляхом узгоджувати національний конституційний порядок із європейським, якщо Конституція забороняє себе змінювати в умовах воєнного стану (ч. 2 ст. 157) [1]. Мета тез – сформулювати аргументовану відповідь на ці питання.

У світовій доктрині конституційна ідентичність розглядається не як статична даність, а як результат діалогу між конституційними прагненнями спільноти та її історичним досвідом [6]. У європейському вимірі ця ідея пов'язана з тлумаченням ч. 2 ст. 4 ДЄС: А. фон Богданді та С. Шилль вбачають

у ній інструмент відмови від абсолютного примату та водночас засіб конституційного плюралізму в межах права ЄС [7]; П. Фарагуна застерігає, що ідентичність може бути як щитом, так і мечем, зокрема для виправдання нелібералізму [8]. Практика Суду ЄС показує межі «щита»: у справі *Melloni* вищий національний стандарт захисту прав не допускається, якщо він ставить під загрозу примат, єдність і ефективність права Союзу [9], а у справі *C-430/21* підкреслено, що посилення на національну ідентичність не виправдовує відступу від примату навіть щодо норм конституційного рівня [10]. Аналогічний баланс вибудовує ЄСПЛ: у справі «*Жданока проти Латвії*» Велика палата допустила врахування історико-політичного контексту держави, але за умови пропорційності обмежень та їх періодичного перегляду [11], тоді як у справі «*Седжич і Финці проти Боснії і Герцеговини*» конституційне закріплення дискримінаційного порядку не було визнано виправданням [12].

В Україні зміни 2019 р. закріпили в Преамбулі Конституції європейську ідентичність Українського народу та незворотність європейського курсу, а у ст. 85, 102 і 116 – відповідні повноваження Верховної Ради, Президента та Уряду [1; 2]. Конституційний Суд України (КСУ) у Висновку № 3-в/2018 визнав відповідний законопроект таким, що відповідає вимогам ст. 157 і 158 Конституції [13]. Дослідники розрізняють широке й вузьке розуміння конституційної ідентичності та пов'язують її з установчою владою [14, с. 69-88]; вказують на ризик використання ідентичності для уникнення примату міжнародного права [15]; трактують її як відображення національної ідентичності в тексті Конституції, що фіксує цінності, які спільнота вважає фундаментальними [16, с. 3-14]. На договірному рівні повага до демократії, прав людини та верховенства права є істотними елементами Угоди про асоціацію [17, ст. 2]. Однак попри вагомий напружений брак аналізу того, як

конституційне «ядро» співвідноситься з процедурними обмеженнями конституційного процесу за воєнного стану та з вимогами вступу.

Вважаю, що конституційну ідентичність України в контексті євроінтеграції слід розуміти як «відкриту, але не безмежну»: європейський вектор є складовою самої ідентичності, а її захист має бути діалогічним, а не вето-подібним. Це обґрунтовується трьома аргументами.

По-перше, оскільки європейський вибір прямо закріплений у конституційному тексті [1; 2], протиставлення «національної ідентичності» та «європейської інтеграції» є хибним. Реальна напруга виникає між ядром і периферією ідентичності. Ядро доцільно визначати через конституційні межі перегляду Конституції: засади суверенітету й територіальної цілісності, права і свободи людини (ст. 157) та особливий порядок зміни розділів I, III і XIII (ст. 156) [1]. Ці елементи значною мірою збігаються з цінностями ст. 2 ДЄС – гідністю, свободою, демократією, рівністю, верховенством права та правами людини [5]. Така «конвергенція ядер» робить справжній конфлікт винятком. Периферію становлять інституційні рішення, що можуть і повинні адаптуватися. Приклад – виборчі права: ст. 38 і 70 Конституції пов’язують їх із громадянством, тоді як ст. 22 Договору про функціонування ЄС надає громадянам Союзу право голосу на місцевих виборах за місцем проживання [1; 5]. Придатною технікою такої адаптації є точкова зміна Конституції, подібна до тієї, що була застосована щодо юрисдикції Міжнародного кримінального суду (ст. 124) [1].

По-друге, головний ризик має процедурний, а не ціннісний характер. Відповідно до ст. 9 Конституції укладення міжнародного договору, який їй суперечить, можливе лише після внесення відповідних змін [1], а ч. 2 ст. 157 забороняє змінювати Конституцію за воєнного стану. Виникає «пастка

послідовності»: договір про вступ не може бути ратифікований до конституційних адаптацій, а вони – до припинення воєнного стану. Її не можна розв’язати ні ігноруванням ст. 157, ні розширювальним тлумаченням «ідентичності» як підстави для відмови від зобов’язань. Вихід полягає в завчасній підготовці пакета адаптацій (з попереднім висновком КСУ згідно зі ст. 159 [1]) та у «євроінтеграційно-дружньому» тлумаченні чинних норм у межах ядра.

По-третє, ідентичність дедалі більше співвиробляється разом із європейськими інституціями. У висновку 2022 р. Європейська комісія серед умов просування назвала реформу відбору суддів КСУ відповідно до рекомендацій Венеційської комісії та оновлення законодавства про національні меншини [3]; відповідні закони було ухвалено в грудні 2022 р. [18; 19]. Показовим є й мовне питання. КСУ підтвердив конституційність закону про державну мову, виходячи зі статусу української мови за ст. 10 Конституції [20], і в літературі це рішення розглядають як приклад звернення до логіки конституційної ідентичності [14]. Водночас Венеційська комісія вказувала на недостатність захисту мов національних меншин [21]. Мій висновок: захист державної мови є легітимним елементом ядра, проте його реалізація має відповідати критеріям пропорційності, що впливають із практики ЄСПЛ [11]; інакше «щит» ідентичності перетвориться на джерело вразливості в переговорах.

Європеїзація конституційного тексту не є новим явищем. У справі «Олександр Волков проти України» ЄСПЛ констатував порушення права на справедливий суд у процедурі звільнення судді та вказав на системні проблеми судової дисциплінарної системи [22]. Ці висновки, разом з оцінками Венеційської комісії щодо проєкту змін до Конституції в частині правосуддя

[23], можна розглядати як складову контексту конституційної реформи 2016 р. [24]. Отже, європейські стандарти вже виступали не зовнішнім тиском, а джерелом змістовного оновлення конституційного ладу, яке не зруйнувало його ядра.

Окремого врахування потребує воєнний вимір. Повномасштабна агресія зробила питання ідентичності не суто академічним: під час форуму за участі Офісу Ради Європи в Україні суддя ЄСПЛ від України М. Гнатовський наголосив, що конституційну ідентичність і європейські цінності не слід протиставляти [25]. Ця позиція узгоджується з розумінням ідентичності як відображення цінностей, які спільнота вважає фундаментальними [16, с. 3–14]. Для практики звідси випливає, що війна посилює легітимність захисту суверенітету й територіальної цілісності як ядра, але не створює підстав для відмови від європейських стандартів захисту прав людини.

Можливе заперечення полягає в тому, що клаузула ідентичності має слугувати жорстким бар'єром проти «розчинення» національного конституційного порядку в праві Союзу. Проте така версія доктрини, як показує критика П. Фарагуни [8] та позиція Суду ЄС [10], є непереконливою для держави, яка лише готується до членства: вона не забезпечує реального захисту, а лише підриває довіру партнерів. Водночас мінімальна гарантія є легітимною, адже сам ДЄС визнає значення національних ідентичностей [5]. Тому доцільно закріпити не право вето, а процедуру аргументованого діалогу, за якої твердження про порушення ядра має бути доведене за прозорими критеріями.

Важливо і те, що КСУ вже має інструментарій для такої роботи. Розглядаючи законопроект про європейський і євроатлантичний курс, Суд перевіряв його саме крізь призму меж перегляду Конституції, тобто крізь ст. 157 і 158 [13]; отже, на практиці «конституційне ядро» вже виступає критерієм

допустимості змін. Крім того, згідно зі ст. 151 Конституції Суд може надавати висновок щодо відповідності Конституції міжнародних договорів, що вносяться до парламенту для надання згоди на обов'язковість [1]. Це створює основу для попереднього конституційного контролю договору про вступ, який не вимагатиме нових інститутів і водночас гарантуватиме правову визначеність для ЄС.

Конституційна ідентичність України має відкритий характер: європейський вибір є її конституційно закріпленим елементом, а «тверде ядро» збігається з ключовими цінностями ЄС. Основна проблема полягає не в ціннісній несумісності, а в послідовності процедур (ст. 9 і ч. 2 ст. 157 Конституції). З метою вдосконалення законодавства та правозастосовної практики пропонується таке.

Перше: передбачити в Конституції «інтеграційне положення», що допускало б передачу частини повноважень наднаціональним органам на підставі договору, який ратифікується кваліфікованою більшістю, із застереженням про недоторканність засад, визначених розділом I та ст. 157. Друге: завчасно підготувати із залученням Венеційської комісії пакет конституційних адаптацій (зокрема щодо ст. 38, 70 і положень про судоустрій) для ухвалення після припинення воєнного стану. Третє: КСУ доцільно виробити методологію ідентифікації конституційного ядра за критеріями зв'язку з установчою владою народу, закріплення у ст. 156–157 та збігу з цінностями ст. 2 ДЄС, використовуючи «ідентифікаційні» аргументи лише у взаємодії з практикою ЄСПЛ і Суду ЄС. Четверте: судам і органам публічної влади застосовувати «євроінтеграційно-дружнє» тлумачення національного права там, де це не виходить за межі конституційного ядра. П'яте: використати ст. 151 Конституції для попереднього контролю договору про вступ до ЄС, поєднавши

його з розробленою КСУ методологією, що дозволить виявити колізії до ратифікації, а не після неї [1].

Список використаних джерел

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 30.09.2026).
2. Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору) : Закон України від 07.02.2019 № 2680-VIII. Відомості Верховної Ради України. 2019. № 9. Ст. 50. URL: <https://zakon.rada.gov.ua/laws/show/2680-19> (дата звернення: 30.09.2026).
3. European Commission. Commission Opinion on Ukraine's Application for Membership of the European Union : Communication from the Commission to the European Parliament, the European Council and the Council, COM(2022) 407 final. Brussels, 17.06.2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0407> (дата звернення: 30.09.2026).
4. European Council. European Council Meeting (14 and 15 December 2023) – Conclusions : EUCO 20/23. Brussels, 15.12.2023. URL: <https://www.consilium.europa.eu/media/68967/europeancouncilconclusions-14-15-12-2023-en.pdf> (дата звернення: 30.09.2026).
5. Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Official Journal of the European Union. 2016. C 202. 07.06.2016. P. 1–388. URL:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016ME/TXT> (дата звернення: 30.09.2026).

6. Jacobsohn G. J. *Constitutional Identity*. Cambridge, MA ; London : Harvard University Press, 2010. DOI: <https://doi.org/10.4159/9780674059399>.

7. von Bogdandy A., Schill S. *Overcoming Absolute Primacy: Respect for National Identity under the Lisbon Treaty*. *Common Market Law Review*. 2011. Vol. 48, № 5. P. 1417–1454. DOI: <https://doi.org/10.54648/COLA2011057>. URL: <https://handle.uba.uva.nl/personal/search?identifier=b2821aa5-e874-4892-89f1-5d70714fbdb3> (дата звернення: 30.09.2026).

8. Faraguna P. *Constitutional Identity in the EU – A Shield or a Sword?* *German Law Journal*. 2017. Vol. 18, № 7. P. 1617–1640. DOI: <https://doi.org/10.1017/S207183220002246X>. URL: <https://www.cambridge.org/core/journals/german-law-journal/article/constitutional-identity-in-the-eua-shield-or-a-sword/D69EB720BC6E49B26E79B80433DCEB03> (дата звернення: 30.09.2026).

9. Judgment of the Court of Justice of the European Union (Grand Chamber) of 26 February 2013 in Case C-399/11, Stefano Melloni v Ministerio Fiscal. ECLI:EU:C:2013:107. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62011CJ0399> (дата звернення: 30.09.2026).

10. Judgment of the Court of Justice of the European Union (Grand Chamber) of 22 February 2022 in Case C-430/21, Proceedings Brought by RS. ECLI:EU:C:2022:99. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0430> (дата звернення: 30.09.2026).

11. Ždanoka v. Latvia : judgment of the ECtHR (Grand Chamber) of 16.03.2006, application no. 58278/00. HUDOC. URL: <https://hudoc.echr.coe.int> (дата звернення: 30.09.2026).

12. Sejdić and Finci v. Bosnia and Herzegovina : judgment of the ECtHR (Grand Chamber) of 22.12.2009, applications nos. 27996/06 and 34836/06. HUDOC. URL: <https://hudoc.echr.coe.int> (дата звернення: 30.09.2026).

13. Висновок Конституційного Суду України у справі за конституційним зверненням Верховної Ради України щодо відповідності законопроекту (реєстр. № 9037) вимогам статей 157 і 158 Конституції України : від 22.11.2018 № 3-в/2018. URL: <https://ccu.gov.ua> (дата звернення: 30.09.2026).

14. Колісник В. П., Берченко Г. В., Слінько Т. М. Конституційна ідентичність як втілення установчої влади. Вісник Національної академії правових наук України. 2022. Т. 29. № 3. С. 69–88. DOI: <https://doi.org/10.31359/1993-0909-2022-29-3-69>. URL: https://ccu.gov.ua/sites/default/files/library/kolisnyk_v.p._konstytuciyna_identychnist_yak_vtillennya_ustanovchoyi_vlady_2022.pdf (дата звернення: 30.09.2026).

15. Никорак О. Ю. Конституційна ідентичність як категорія конституційного права : дис. ... д-ра філософії : 081 «Право» / Львівський національний університет імені Івана Франка. Львів, 2023. 248 с. URL: <https://repository.lnu.edu.ua/handle/123456789/1419> (дата звернення: 30.09.2026).

16. Бориславська О. М. Концепт конституційної ідентичності: між викликами війни та вимогами європейської інтеграції. Український часопис конституційного права. 2025. № 3. С. 3–14. DOI: <https://doi.org/10.30970/jcl.3.2025.1>. URL: <https://www.constjournal.com/wp-content/uploads/issues/2025-3/pdfs/1-olena-borysl>

avska-kontsept-konstytutsiinoi-identychnosti-mizh-vyklykamy-viiny-vymohamy-yevropeiskoi.pdf (дата звернення: 30.09.2026).

17. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : міжнародний договір від 27.06.2014, ратифікований Законом України від 16.09.2014 № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 30.09.2026).

18. European Commission for Democracy through Law (Venice Commission). Ukraine – Opinion on the Draft Law “On Amending Some Legislative Acts of Ukraine Regarding Improving Procedure for Selecting Candidate Judges of the Constitutional Court of Ukraine on a Competitive Basis” : Opinion No. 1109/2022, CDL-AD(2022)054, adopted at the 133rd Plenary Session (Venice, 16–17 December 2022). Strasbourg, 19.12.2022. URL: <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282022%29054-e> (дата звернення: 30.09.2026)

19. Про національні меншини (спільноти) України : Закон України від 13.12.2022 № 2827-IX. URL: <https://zakon.rada.gov.ua/laws/show/2827-20> (дата звернення: 30.09.2026).

20. Рішення Конституційного Суду України у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України «Про забезпечення функціонування української мови як державної» : від 14.07.2021 № 1-п/2021. URL: <https://zakon.rada.gov.ua/laws/show/v001p710-21> (дата звернення: 30.09.2026).

21. European Commission for Democracy through Law (Venice Commission). Ukraine – Opinion on the Law on Supporting the Functioning of the Ukrainian Language as the State Language : CDL-AD(2019)032, adopted at the 121st

Plenary Session (Venice, 6–7 December 2019). Strasbourg, 09.12.2019. URL: <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282019%29032-е> (дата звернення: 30.09.2026).

22. Oleksandr Volkov v. Ukraine : judgment of the European Court of Human Rights (Fifth Section) of 09.01.2013, application no. 21722/11, final on 27.05.2013. URL: https://zakon.rada.gov.ua/laws/show/974_947 (дата звернення: 30.09.2026).

23. European Commission for Democracy through Law (Venice Commission). Ukraine – Opinion on the Proposed Amendments to the Constitution of Ukraine regarding the Judiciary as Approved by the Constitutional Commission on 4 September 2015 : CDL-AD(2015)027, adopted at the 104th Plenary Session (Venice, 23–24 October 2015). Strasbourg, 26.10.2015. URL: <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282015%29027-е> (дата звернення: 30.09.2026).

24. Про внесення змін до Конституції України (щодо правосуддя) : Закон України від 02.06.2016 № 1401-VIII. URL: <https://zakon.rada.gov.ua/laws/show/1401-19> (дата звернення: 30.09.2026).

25. Українська конституційна ідентичність та європейська інтеграція: пошук балансу. Офіс Ради Європи в Україні. URL: <https://www.coe.int/uk/web/kyiv/-/ukrainian-constitutional-identity-and-european-integration-finding-a-balance> (дата звернення: 30.09.2026).

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 341.231.14:342.7

СИСТЕМА ПРАВОВИХ СТАНДАРТІВ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ

Гелетій Микола Володимирович

аспірант Інституту права, психології та інноваційної освіти

НУ «Львівська політехніка»

м. Львів, Україна

Захист прав людини є її перманентним правом та повинно забезпечуватися з боку держави, міжнародних інституцій та всього цивілізованого суспільства.

В умовах воєнного стану, загроз для цивільного населення, порушення правил ведення військових дій, проблем інфраструктурного характеру є загроза для життя та здоров'я населення й гарантувати повноцінний захист громадян державна влада не завжди спроможна.

Проте вагомим залишається принцип державного захисту прав та свобод людини та громадянина навіть в умовах повномасштабної війни, оскільки такий ціннісний підхід відображає як функціональне підґрунтя правової держави, так і державно-управлінської діяльності.

На сучасному етапі розвитку доктринальної думки та міжнародно-правових стандартів слід говорити про формування цілої системи міжнародного захисту – інститут міжнародного гуманітарного права. Такий інститут містить положення, що унормовує суспільні відносини під час війни, правила, принципи та стандарти ведення збройного конфлікту тощо.

Основними джерелами унормування інституту міжнародного-гуманітарного права є Женевські конвенції 1949 року та Додаткові протоколи до них 1977 року. Вони визначають правила захисту військовополонених, комбатантів, що поранені, і звісно цивільного населення.

Разом з тим державна влада та суспільство воюючої держави використовує сталі правові конституційні принципи національного законодавства, проте модифікуючи їх під військово політичну реальність.

В Україні правові засади забезпечення прав і свобод людини в умовах воєнного стану визначаються Конституцією України, Законом України «Про правовий режим воєнного стану», іншими нормативно-правовими актами та міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України.

Відповідно до статті 64 Конституції України, в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку їх дії. Водночас Конституція визначає перелік прав, які не можуть бути обмежені навіть за таких обставин.

Обмеження прав – це правомірна, легітимна та й, так би мовити, звична практика в кризових умовах конвенційного характеру. Проте вагомо, щоб такі обмеження мали збалансований характер, вони «мають залишатися правомірними, пропорційними та відповідати національному законодавству, Європейській конвенції з прав людини та міжнародним стандартам» [1].

Разом з тим в такій системі механізмів захисту в умовах особливо дисбалансу державного механізму прослідковуються суттєві прогалини в правореалізаційній практиці. Задекларовані незмінні правові стандарти часто стають приводом до маніпуляцій та зловживання права. Професор Наталія Маслова з цього приводу справедливо зауважує, що «попри існування правових

норм щодо обмеження прав і свобод під час воєнного стану, відсутність чітких механізмів їхньої реалізації призводить до правової невизначеності, зниження ефективності правозахисної діяльності та ризику зловживання владою» [2].

Тому узагальнюючи викладене доречно вказати, що система правових стандартів захисту прав людини в умовах воєнного стану містить тріаду нормативно-правових еталонів, зокрема норм міжнародного гуманітарного права, міжнародного та європейського (регіонального) права у сфері прав людини та національного законодавства, що адаптовано під відповідні воєнні виклики. Вагомо оптимально забезпечити взаємодію та поєднання визначених стандартів з метою гарантування механізму захисту прав та свобод громадян.

Список використаних джерел:

1. Ніколенко Л.М. Захист прав людини в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. №1 (91), С. 207-212. DOI: <https://doi.org/10.24144/2307-3322.2025.91.1.30>
2. Маслова Н.Г. Проблеми дотримання прав людини в умовах воєнного стану на прикладі України. *Український політико-правовий дискурс*. 2025. № 13. DOI: <https://doi.org/10.5281/zenodo.15825983>

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.7:342.76(477)

КОНСТИТУЦІЙНІ МЕЖІ ОБМЕЖЕННЯ ПРАВ І СВОБОД ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ

Готра Вікторія Віталіївна,
студентка 2 курсу магістратури (2 група),
заочної форми навчання,
спеціальності D8 Право,
Ужгородський університет

Права і свободи людини є однією з основ конституційного ладу України, а їх утвердження і забезпечення відповідно до статті 3 Конституції України є головним обов'язком держави [1]. В умовах воєнного стану держава об'єктивно стикається з необхідністю застосування спеціальних заходів для забезпечення оборони, національної безпеки, захисту життя і здоров'я населення. Вказані заходи можуть передбачати тимчасове обмеження окремих прав і свобод людини, що породжує проблему визначення допустимих меж державного втручання.

Актуальність дослідження зумовлена необхідністю забезпечення балансу між інтересами національної безпеки та гарантуванням прав людини. Як зазначає Д.Д. Гриньо, обмеження прав і свобод у період воєнного стану має здійснюватися виключно на правовій основі, з урахуванням загального інтересу та необхідності встановлення справедливого балансу між публічними і приватними інтересами [8, с. 45-46]. Отже, саме існування воєнного стану не може розглядатися як підстава для необмеженого втручання держави у сферу прав людини.

Конституційною основою обмеження прав і свобод в умовах воєнного стану є стаття 64 Конституції України. Відповідно до її цієї статті,

конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. Водночас в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку їх дії. Стаття 64 Конституції України встановлює перелік прав і свобод, які не можуть бути обмежені навіть в умовах воєнного або надзвичайного стану [1]. Конституція України передбачає дворівневий механізм захисту прав людини. З одного боку, допускається тимчасове обмеження окремих прав за надзвичайних умов, а з іншого - встановлюється категорія прав, щодо яких таке обмеження прямо заборонене. Науковці звертають увагу на те, що український перелік прав, які не підлягають обмеженню відповідно до статті 64 Конституції України, є ширшим порівняно з мінімальними міжнародними стандартами [8, с. 46].

Спеціальним нормативно-правовим актом у цій сфері є Закон України «Про правовий режим воєнного стану». Відповідно до статті 1 цього Закону воєнний стан є особливим правовим режимом, який, зокрема, передбачає можливість тимчасового обмеження конституційних прав і свобод людини і громадянина із зазначенням строку дії цих обмежень [2]. Стаття 6 Закону встановлює вимогу щодо зазначення в указі Президента України про введення воєнного стану переліку конституційних прав і свобод, які тимчасово обмежуються, а також строку дії таких обмежень [2].

Важливе значення мають і міжнародно-правові стандарти. Стаття 15 Конвенції про захист прав людини і основоположних свобод передбачає можливість відступу держави від виконання окремих зобов'язань під час війни або іншої суспільної небезпеки, яка загрожуює життю нації, але лише тією мірою, якою цього вимагає гострота становища [4]. Подібний механізм передбачений статтею 4 Міжнародного пакту про громадянські і політичні права [5].

У сучасній юридичній науці наголошується на тому, що введення воєнного стану не означає повного припинення реалізації прав і свобод людини. Д. Б. Ступак та О. О. Шевчук зазначають, що обмеження мають здійснюватися виключно в межах, визначених Конституцією та законами України, із дотриманням принципів пропорційності, необхідності та недискримінації [10, с. 453]. Автори також акцентують увагу на значенні «ядерних» прав, які не можуть бути обмежені відповідно до статті 64 Конституції України [10, с. 453-454].

На нашу думку, конституційні межі обмеження прав і свобод людини в умовах воєнного стану необхідно визначати не лише через встановлений Конституцією перелік прав, які можуть або не можуть бути обмежені. Важливе значення має також оцінка самого способу, мети, строку та інтенсивності втручання держави у відповідне право.

Першою та основною межею є законність. Обмеження конституційного права повинно мати належну правову основу та здійснюватися компетентним суб'єктом у межах наданих йому повноважень. Сам факт запровадження воєнного стану не надає органам державної влади необмеженої дискреції щодо визначення обсягу прав людини. Такий підхід відповідає як Конституції України, так і міжнародним стандартам прав людини. Д. Д. Гриньо звертає увагу на необхідність чіткого та доступного нормативного регулювання обмежень, оскільки відсутність належної визначеності може створювати можливості для надмірного розсуду органів публічної влади [8, с. 46-47].

Другою межею є тимчасовість обмеження. Частина перша статті 64 Конституції України прямо вимагає зазначення строку дії обмежень [1]. Отже, обмеження не може встановлюватися безстроково або продовжуватися без належного обґрунтування необхідності його подальшого застосування.

Тимчасовість у цьому випадку має розглядатися не лише як формальне зазначення дати припинення обмеження, а і як вимога постійної оцінки того, чи зберігаються обставини, які зумовили необхідність такого втручання.

Третьою межею є легітимна мета та необхідність. Обмеження прав людини повинно бути спрямоване на досягнення конституційно значущої мети, зокрема забезпечення оборони держави, національної безпеки, громадської безпеки або захисту прав інших осіб. Водночас сама по собі наявність легітимної мети не може автоматично виправдовувати будь-яке втручання у право.

Четвертою межею є пропорційність (домірність). Втручання держави має відповідати характеру та масштабам загрози, а обраний захід не повинен створювати надмірного тягаря для особи. У науковій літературі принцип пропорційності розглядається як один із ключових критеріїв допустимості обмеження прав людини в умовах воєнного стану [10, с. 453-456]. Аналогічний підхід впливає з практики Європейського суду з прав людини, відповідно до якої втручання у права має бути передбачене законом, переслідувати легітимну мету та бути необхідним у демократичному суспільстві [8, с. 46-47].

Особливого значення для визначення меж обмеження прав людини набуває практика Конституційного Суду України. У Рішенні від 18 липня 2024 року № 8-р(II)/2024 Суд наголосив, що навіть в умовах воєнного стану верховенство Конституції України, принцип верховенства права та повага до прав і свобод людини залишаються основами демократичного конституційного ладу [6]. Вказане положення отримало подальший розвиток у Рішенні Конституційного Суду України від 19 травня 2026 року № 3-р/2026. Суд зазначив, що механізм обмеження конституційних прав і свобод, передбачений статтею 64 Конституції України, діє і в умовах воєнного стану, однак обмеження

не може нівелювати сутність права або посягати на мінімальні гарантії його реалізації [7]. Конституційний Суд також наголосив на необхідності врахування домірності обраних законодавцем засобів та недопустимості зниження рівня конституційних гарантій до такого ступеня, за якого право фактично перестає реалізовуватися. Так, навіть щодо прав, які відповідно до статті 64 Конституції України можуть бути обмежені, держава не отримує права фактично скасувати їх або позбавити особу мінімально необхідної можливості їх реалізації.

П'ятою межею є збереження сутності права та людської гідності. Частина перша статті 3 Конституції України визначає людину, її життя і здоров'я, честь і гідність, недоторканність та безпеку найвищою соціальною цінністю [1]. Тому будь-яке обмеження прав людини має здійснюватися таким чином, щоб не перетворювати особу виключно на об'єкт державного управління. Як зазначають Д. Б. Ступак та О. О. Шевчук, людська гідність має виступати одним із ключових орієнтирів при визначенні допустимого обсягу державного втручання в умовах воєнного стану [10, с. 455-456].

Окремо слід наголосити на судовому контролі як важливій гарантії дотримання конституційних меж. Право на судовий захист передбачене статтею 55 Конституції України та відповідно до частини другої статті 64 належить до прав, які не можуть бути обмежені в умовах воєнного стану [1]. Саме судовий контроль дає можливість перевірити, чи діяли органи державної влади в межах компетенції, чи мали застосовані заходи належну правову основу та чи не було втручання у права особи надмірним.

Вважаємо, що сукупність таких критеріїв, як законність, легітимна мета, необхідність, пропорційність, тимчасовість, юридична визначеність, збереження сутності права та можливість судового контролю, повинна становити основу оцінки допустимості будь-якого обмеження прав і свобод

людини в умовах воєнного стану. При цьому наявність воєнного стану не повинна розглядатися як самостійне виправдання будь-якого обмеження.

Відтак, Конституція України допускає можливість тимчасового обмеження окремих прав і свобод людини в умовах воєнного стану, однак така можливість має чіткі конституційні межі. Держава зобов'язана діяти на підставі та в межах Конституції і законів України, встановлювати обмеження на визначений строк та забезпечувати їх відповідність легітимній меті й принципу пропорційності [1; 2]. Особливе значення має частина друга статті 64 Конституції України, яка встановлює перелік прав і свобод, що не можуть бути обмежені в умовах воєнного стану [1]. Водночас практика Конституційного Суду України свідчить, що навіть щодо прав, які можуть бути обмежені, держава не може нівелювати їх сутність або знижувати мінімальні гарантії їх реалізації [7].

Для вдосконалення механізму захисту прав людини в умовах воєнного стану доцільно забезпечити більш чітку нормативну конкретизацію критеріїв законності, необхідності та пропорційності обмежень, а також ефективний судовий контроль за рішеннями і діями органів публічної влади. Такий підхід дозволить забезпечити необхідний баланс між потребами національної безпеки та конституційним обов'язком держави гарантувати права і свободи людини.

Список використаних джерел

1. Конституція України: Закон України від 28 червня 1996 року №254к/96-ВР; URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 24.09.2026)

2. Про правовий режим воєнного стану: Закон України від 12 травня 2015 року № 389-VIII. URL: <https://zakon.rada.gov.ua/laws/show/389-19> (дата звернення: 24.09.2026)

3. Про продовження строку дії воєнного стану в Україні : Указ Президента України від 13 липня 2026 року №596/2026; URL: <https://www.president.gov.ua/documents/5962026-60509> (дата звернення: 24.09.2026)

4. Конвенція про захист прав людини і основоположних свобод: від 4 листопада 1950 року. (з поправками). Ратифікована Законом України від 17.07.1997 №475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 24.09.2026)

5. Міжнародний пакт про громадянські і політичні права: прийнятий 16 грудня 1966 року Генеральною Асамблеєю ООН No 2148-VIII. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 24.09.2026)

6. Рішення Конституційного Суду України від 18 липня 2024 року № 8-р(II)/2024 у справі щодо гарантій судового контролю за дотриманням прав осіб, яких утримують під вартою; URL: <https://ccu.gov.ua/dokument/8-rii2024> (дата звернення: 24.09.2026)

7. Рішення Конституційного Суду України від 19 травня 2026 року №3-р/2026 у справі щодо права на відпустки в умовах воєнного стану; URL: <https://zakon.rada.gov.ua/laws/show/va03p710-26> (дата звернення: 24.09.2026)

8. Гриньо Д. Д. Обмеження прав і свобод людини в умовах воєнного стану в Україні. Часопис Київського університету права. 2023. № 2. DOI: 10.36695/2219-5521.2.2023.08; URL:

<https://chasprava.com.ua/index.php/journal/article/view/853> (дата звернення: 24.09.2026)

9. Полховська І. К. Реалізація прав і свобод особи в умовах воєнного стану. Полтавський правовий часопис. 2022. № 2. DOI: 10.21564/2786-7811.2.287927; URL: <https://plr.nlu.edu.ua/article/view/287927> (дата звернення: 24.09.2026)

10. Ступак Д. Б., Шевчук О. О. Конституційні гарантії та допустимі обмеження прав і свобод людини та громадянина в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право. 2026. Т. 2, № 94. DOI: 10.24144/2307-3322.2026.94.2.65. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/364603> (дата звернення: 24.09.2026)

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.56:347.97/.99(477)

КОНСТИТУЦІЙНО-ПРАВОВИЙ СТАТУС СУДУ ПРИСЯЖНИХ ЯК ФОРМИ УЧАСТІ НАРОДУ У ЗДІЙСНЕННІ СУДОВОЇ ВЛАДИ

Грига Наталія Вікторівна,
студентка 2-го курсу ОС "Магістр"
заочної форми навчання,
спеціальності D8 Право,
Ужгородський університет

У сучасному демократичному суспільстві правосуддя не може вважатися цілком ефективним та справедливим, якщо воно ізольоване від залучення громадськості. Конституційно-правовий статус суду присяжних є одним із найважливіших інститутів, який забезпечує безпосередню участь народу у здійсненні судової влади. Завдяки цій формі народовладдя громадяни беруть пряму участь у відправленні правосуддя, що слугує дієвим гарантом його неупередженості, прозорості та незалежності. З моменту конституційного закріплення і по сьогоднішнього відбувається пошук оптимальної моделі суду присяжних.

В українській моделі суд присяжних складається з двох професійних суддів та трьох присяжних, які спільно вирішують питання факту та права. Така модель відрізняється від класичної англо-американської системи, де присяжні самостійно вирішують питання факту, а суддя – питання права. Справи за участю присяжних розглядаються в першій інстанції лише у випадках, коли обвинуваченому загрожує довічне позбавлення волі, і лише за клопотанням обвинуваченого. Присяжним може бути громадянин України, який досяг тридцятирічного віку і постійно проживає на території, на яку поширюється

юрисдикція відповідного суду. Існує ряд обмежень щодо того, хто не може бути присяжним: особи з непогашеною судимістю, недієздатні особи, особи з хронічними психічними чи іншими захворюваннями, що перешкоджають виконанню обов'язків присяжного, особи старші 65 років, народні депутати, члени Кабінету Міністрів України, судді, прокурори, працівники правоохоронних органів та інші [1, ст. 15].

Закріплене в ст. 38 Конституції України [2] право громадян керувати державою охоплює не лише формування виконавчої та судової гілок влади, а й безпосередню участь у їхній роботі. Щодо виконавчих органів це виявляється передусім у спроможності громадян впливати на ухвалення рішень, тоді як демократичний устрій передбачає їхнє залучення до створення судової системи та здійснення правосуддя.

Вдосконалення форм участі громадян в управлінні державними справами у сфері судової влади обумовлює необхідність розмежування таких юридичних конструкцій: «участь громадян у здійсненні правосуддя» та «участь громадян в організації судової влади». Участь громадян у діяльності судової влади відображає непряму участь у відправленні правосуддя і спрямована на залучення громадян у процес формування та діяльності судових органів [3, ст. 49].

Варто зазначити, що законодавець передбачив участь присяжних лише в деяких категоріях справ, оскільки вони є особливо складними й зачіпають особисті немайнові права людини. Але інші справи окремого провадження, на її думку, теж пов'язані з особистими немайновими правами фізичних осіб. Наприклад, справи про емансипацію, про надання права на шлюб, про розірвання шлюбу за заявою подружжя, яке має дітей, про встановлення режиму окремого проживання за заявою подружжя. Проте вони розглядаються

суддею одноособово, хоча теж є досить складними і вимагають детального розгляду та вивчення для ухвалення законного та обґрунтованого рішення. У таких категоріях справ захищаються як майнові, так і немайнові особисті права особи [4, ст.70].

Водночас суттєвою перешкодою для українського судочинства залишається надмірна завантаженість місцевих судів, що призводить до систематичного порушення розумних строків розгляду справ. Повноцінний запуск суду присяжних ризикує додатково ускладнити цю ситуацію, оскільки вимагатиме значного часу на відбір кандидатів, їхнє інструктування, детальний аналіз доказів та проведення нарад.

Отже, саме Конституція України вирішує проблему співвідношення народного суверенітету і державної влади шляхом формулювання суверенітету народу як найважливішого принципу організації та діяльності органів державної влади, як принципу конституційного ладу України (ст. 5 Конституції України). Це свідчить про похідний характер влади державних органів: джерело влади органів державної влади та органів місцевого самоврядування не в них самих, а у волі Українського народу. Тому держава не повинна виступати як ізольований та незалежний від народу носій державної влади, вона є інструментом здійснення самодержавства народу, його верховенства та повновладдя. Більш того, на території всієї країни, як це встановлено чинною Конституцією України, діє державна влада. Її джерело – народ країни [3, ст. 49].

Вважаємо, що в березні 2025 року, коли Верховна Рада України проголосувала в першому читанні законопроект про запровадження в Україні суду присяжних, було остаточно закріплено базові підходи до української моделі суду присяжних. Майбутня українська модель суду присяжних матиме характер, наближений до англосаксонської моделі, за якою суд присяжних

складатиметься з одного професійного судді та лави присяжних. Так, в проєкті закону «Про суд присяжних» [5] в ст. 3 «Склад суду присяжних» передбачено, що «Суд присяжних складається з одного професійного судді і лави присяжних. Професійний суддя суду присяжних є процесуальним головуючим у судовому засіданні та не бере участі в прийнятті рішення Лавою присяжних по суті обвинувачення особи у вчиненні діяння, передбаченого Кримінальним кодексом України [6, ст. 35].

З вище наведеного можна зробити висновок, що головна цінність цього законопроекту полягає у чіткому розмежуванні ролей: суддя керує процесом, а пересічні громадяни самостійно вирішують долю обвинуваченого, без жодного тиску чи підказок з боку системи.

У результаті дослідження вдалося сформулювати цілісний підсумок цієї проблематики. Суд присяжних є безпосереднім проявом народного суверенітету та ключовим гарантом прозорості, неупередженості й незалежності правосуддя, оскільки залучення громадян до відправлення судової влади виступає важливим чинником відновлення суспільної довіри до судочинства. Аналіз практики застосування чинних норм переконливо свідчить про необхідність остаточного відходу від діючої шефенської моделі, яка зводить участь громадян до формальної присутності поруч із професійними суддями та нівелює їхню автономію.

Стратегічним вектором законодавчої трансформації є перехід до класичної англосаксонської моделі з чітким розмежуванням компетенцій, де лава присяжних одноосібно ухвалює вердикт щодо винуватості особи, а професійний суддя здійснює процесуальне керівництво та призначає покарання. Ефективність функціонування цього інституту вимагає узгодженого застосування трьох системних груп норм – інституційно-матеріальних,

процедурних та процесуальних. Перспективи подальшого розвитку полягають у цифровізації процедур відбору кандидатів, поступовому розширенні юрисдикції суду присяжних та гарантуванні належного соціально-правового захисту присяжних, що дозволить мінімізувати ризики процесуального затягування справ і надмірного навантаження на судову систему.

Список використаних джерел

1. Богданов Є. А. Інститут присяжних в Україні: сучасні виклики та перспективи реформування. *Експерт: парадигми юридичних наук і державного управління*. 2024. № 4 (32). С. 13–18. URL: <https://journals.maup.com.ua/index.php/expert/article/view/4539/4847> (дата звернення: 01.10.2026).
2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 01.10.2026)
3. Щербанюк О. В. Конституційний принцип участі народу у здійсненні правосуддя. *Юридичний науковий електронний журнал*. 2015. № 2. С. 48-51. URL: https://www.lsej.org.ua/2_2015/13.pdf (дата звернення: 01.10.2026).
4. Татулич І. Правовий статус присяжних у цивільному судочинстві. *Підприємництво, господарство і право*. Серія: Цивільне право і процес. 2019. № 12. С. 67–72. URL: <https://dspace.chnu.edu.ua/server/api/core/bitstreams/a0d3f3c0-feddd-432f-bdb7-4a66abd85af9/content> (дата звернення: 01.10.2026).
5. Про проект Закону про суд присяжних : проект Закону України від 14.07.2020 № 3843. *Верховна Рада України*. URL:

https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69465 (дата звернення: 01.10.2026).

6. Макарова О. В. Реформування інституту суду присяжних у контексті міжнародного досвіду. *Науковий вісник Ужгородського національного університету*. Серія: Право. Випуск 94: частина 4. С. 32-40. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/364510/350035> (дата звернення: 01.10.2026).

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

© Грига Н.В., 2026

УДК: 342.1:323.1

НАЦІОНАЛЬНА ТА КОНСТИТУЦІЙНА ІДЕНТИЧНІСТЬ: ТЕОРЕТИЧНІ ЗАСАДИ ДЕТЕРМІНАЦІЇ

Гудим Вікторія Любомирівна,
аспірантка Інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
м. Львів, Україна

Понятійно-категоріальний апарат для сучасної правової думки має вагоме значення, оскільки відображає доктринальне розуміння явищ та процесів правової реальності.

Не менш вагомо визначити взаємодію окремих понять, особливо якщо вони мають спільну сферу суспільних відносин. До таких понять відносяться зокрема «конституційна ідентичність» та «національна ідентичність».

В межах наукових досліджень європейської школи права популярним є тлумачення про те, що взаємозв'язок та взаємодетермінація понять є суттєвою, конституційна та національна ідентичності тісно переплітаються, оскільки національні цінності (такі як мова, культура, традиції тощо) безпосередньо відображені в конституції, зокрема Ева Кшиштофік вказує, що «національна ідентичність виступає базисом формування та подальшого розвитку конституційної ідентичності, хоча вони й не є тотожними» [1].

Для теоретико-правового дослідження пріоритетно визначимося з категоріями.

Професор Олена Богуславська вказує, що «національна ідентичність (чи то національно-етнічна, чи національно-політична) визначає унікальність та самобутність певної спільноти; вона формується під впливом історичного

досвіду, традиції, культури, мови та інших елементів, що забезпечують згуртованість і стійкість нації» [2]. Таким чином це поняття нерозривно пов'язане з нацією, її історичним генезисом та культурно-ментальними чинниками.

В свою чергу відомі сучасні науковці поняття конституційної ідентичності виводять з таких категорій як «конституція» та «конституціоналізм». Зокрема Віталій Ковальчук позиціонує, що «Конституція як основне джерело конституційної ідентичності виражає не лише усталені традиції та культуру народу, а й універсальні цінності конституціоналізму, зокрема права, свободи людини і громадянина» [3]. Отож відповідно до такого розуміння конституційна ідентичність репрезентує сучасні правові стандарти та гуманістичні цінності, що відображені в основному законі.

Досліджувані поняття безумовно мають ряд суттєвих спільностей, оскільки функціонують в одній сфері суспільного життя. Тому, на нашу думку, доречно вказати на такі спільні аспекти конституційної та національної ідентичності.

По-перше, ці дві категорії діють, формуються та функціонують в одній сфері суспільних відносин – це державно-правові відносини, що пов'язані із взаємозв'язком людини та держави, організацією політичної влади, суверенітетом держави, визначенням засад громадського співжиття. Дія на суспільні відносини при цьому досліджуваних категорій є різною, коли національна ідентичність впливає на правовідносини через культурні чинники, то правова - застосовуючи потенціал правових принципів, державних засад та конституційних цінностей.

По-друге, вони відображають спільні ціннісні атрибути суспільства та держави, формують світоглядні позиції людини та спільноти, світоглядні

орієнтири нації та громадянина. Для національної ідентичності цінностями є мова, культура, традиції, пам'ятні дати тощо, то для конституційної – конституційні принципи права, права людини та громадянина.

По-третє, формують уніфікацію спільностей, сприяють об'єднанню спільноти на національно-правовому підґрунті. Коли національна ідентичність об'єднує спільноту за історично-генезисними культурологічними чинниками, то конституційна гуртує націю на аксіологічно-правових засадах – спільних конституційних принципах та цінностях.

По-четверте, створюють основу для національного суверенітету та захисту територіальної цілісності, оскільки утверджують суверенність держави, її самобутність в історичному та політико-правовому розвитку.

Взаєдeterminація понять є обґрунтованою. Однак вести мову про первинність та вторинність категорій ми б не стали. Національна ідентичність так само розвивається, змінюється та векторалізується як і конституційна ідентичність. Обидві категорії змінюються та трансформуються під впливом як внутрішніх, так і зовнішніх чинників. Часто ці чинники є спільними, тому й спрямованість категорій є однаковою, наприклад до таких спільних чинників можуть належити глобалізаційні виклики, суспільно-політичні трансформації, публічно-ідеологічна парадигма.

Вказане обумовлює потребу переосмислення щодо доктринального бачення первинності та вторинності категорій. Дискусійності підлягає такий підхід, оскільки в модерністському розумінні слід говорити про лінійність національних та конституційних процесів та їх єдину векторіальну спрямованість у глобалізаційному суспільстві.

Список використаних джерел:

7. Krzysztofik E. The principle of respect for the member states' national identity with regard to the rights and obligations of migrant citizens of the European Union. *Zbornik radova Pravnog fakulteta*. 2018. № 57 (79). P. 157-170. DOI: <https://doi.org/10.5937/zrpfni1879157K>
8. Boryslavskа О. Концепт конституційної ідентичності: між викликами війни та вимогами європейської інтеграції. *Ukrainian journal of constitutional law*. 2025. № 36 (3). С. 3-14. DOI: <https://doi.org/10.30970/jcl.3.2025.1>
9. Ковальчук В. Конституційна ідентичність та національні цінності в умовах перманентної загрози державності України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. № 86 (1). С. 206-213. DOI: <https://doi.org/10.24144/2307-3322.2024.86.1.30>

Дата першого надходження рукопису до видання: 9.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.7:004.056.5(477)

КОНСТИТУЦІЙНО-ПРАВОВІ ГАРАНТІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВОЇ ДЕРЖАВИ

Дарвай Вікторія Іванівна,
студентка 2-го курсу магістратури,
спеціальність D8 «Право»,
юридичний факультет,
Ужгородський університет,
м. Ужгород, Україна

Цифрова трансформація публічного управління помітно змінила відносини між людиною і державою. Довідку, по яку колись доводилося ходити до кількох установ, сьогодні можна отримати через «Дію» за кілька хвилин, а державні реєстри обмінюються відомостями між собою без участі громадянина. За цією зручністю стоїть постійне збирання, зберігання, поєднання та передання персональних даних. Держава поступово стає найбільшим розпорядником інформації про особу, і відомості, які раніше лежали в паперових архівах різних органів, технічно можна звести в єдиний цифровий профіль людини. Тому загрозу приватності сьогодні створюють не тільки треті особи, які незаконно заволоділи чужими даними. Ризики становить також надмірне збирання, невизначені строки зберігання, непрозорий доступ посадовців до реєстрів, витоки та кібератаки. Воєнний стан ці ризики тільки посилює.

Звідси питання, яке ми ставимо в центр цих тез, чи достатньо конституційних гарантій, сформованих ще для «доцифрової» епохи, щоб захистити людину в цифровій державі, і в якому напрямі їх варто розвивати?

Відправною точкою є стаття 32 Конституції України. Її частина перша забороняє втручання в особисте і сімейне життя, крім випадків, передбачених

Конституцією, а частина друга не допускає збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1]. Цю норму варто читати разом зі статтею 3, яка визнає людину, її права і свободи найвищою соціальною цінністю, та статтею 8 про верховенство права [1].

Конституційний Суд України наповнив вказані положення конкретним змістом. У Рішенні від 20 січня 2012 року № 2рп/2012 Суд визнав інформацію про особисте та сімейне життя особи (персональні дані про неї) конфіденційною, а її збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами без згоди особи – втручанням в її особисте та сімейне життя, допустимим винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [2]. Для цифрової держави з цього випливає простий, але принциповий висновок. Кожна нова електронна послуга чи міжреєстрова взаємодія, яка передбачає обробку даних без згоди особи, є втручанням у її приватне життя, а значить, потребує підстави в законі, легітимної мети та пропорційності.

Тут виникає своєрідний парадокс згоди. Більшість операцій у державних реєстрах здійснюється на підставі закону, а не згоди, і стаття 32 Конституції це дозволяє. Але якщо людина фактично не може відмовитися від обробки своїх даних державою, вимоги до такого закону мають бути вищими: він повинен чітко визначати, які дані збираються, навіщо, хто має до них доступ і скільки часу вони зберігаються. Без цього формула «у випадках, визначених законом» перетворюється на загальний дозвіл для держави.

Гарантії статті 32 Конституції на рівні законодавства розвиває Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. Він закріплює права суб'єкта персональних даних, зокрема право знати про джерела збирання, місцезнаходження своїх даних і мету їх обробки, а також отримувати інформацію про умови надання доступу до них, у тому числі про третіх осіб, яким ці дані передаються (стаття 8). Контроль за дотриманням цього законодавства здійснюють Уповноважений Верховної Ради України з прав людини та суди (стаття 22) [3]. Закон ухвалювали задовго до появи «Дії», і, на мою думку, він погано пристосований до ризиків масштабної обробки даних у державних інформаційних системах. О. Тимошенко звертає увагу, що через законодавче визначення важко розмежувати персональні дані та конфіденційну інформацію про особу, і пропонує вдосконалити поняття «персональні дані» відповідно до Загального регламенту ЄС про захист даних [4, с. 168, 170]. І. Андронов та співавтори оцінюють ситуацію жорсткіше: на їхню думку, законодавство України у сфері захисту персональних даних не відповідає європейським стандартам [5, с. 423].

Європейські стандарти в цій сфері формувалися насамперед у межах Ради Європи. Україна є учасницею Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108), ратифікованої Законом України від 6 липня 2010 року № 2438-VI [6]. Європейський суд з прав людини розглядає захист персональних даних як складову права на повагу до приватного життя за статтею 8 Конвенції про захист прав людини і основоположних свобод. У справі «S. and Marper v. the United Kingdom» Велика палата наголосила, що захист персональних даних має фундаментальне значення для реалізації права на повагу до приватного і сімейного життя [7, п.103]. Суд звернув увагу на загальний і невибірковий характер повноважень

щодо зберігання відбитків пальців, клітинних зразків і профілів ДНК осіб, підозрюваних у вчиненні злочинів, але не засуджених, і визнав, що такий режим не забезпечує справедливого балансу між публічними та приватними інтересами та порушує статтю 8 Конвенції [7, п.119, 125]. Для державних реєстрів урок очевидний: легітимна мета сама по собі не виправдовує безстрокового й недиференційованого накопичення даних.

Узагальнюючи практику ЄСПЛ, О. Тимошенко виокремлює трискладовий тест, а саме: втручання держави у сферу персональних даних має бути передбачене законом, мати легітимну мету та бути пропорційним [4, с. 170]. Ми пропонуємо перекласти цей тест на мову цифрових сервісів і ставити перед запуском кожної нової послуги кілька запитань. Чи є закон, який прямо передбачає таку обробку даних? Чи зрозуміло людині з його тексту, які саме дані про неї оброблятимуться? Чи не можна досягти тієї самої мети з меншим обсягом даних або коротшим строком їх зберігання? Якщо чіткої відповіді немає хоча б на одне з цих запитань, навіть дуже зручна послуга створює ризик непропорційного втручання в приватне життя.

У праві Європейського Союзу ключовим актом є Регламент (ЄС) 2016/679 (GDPR), який прямо називає своєю метою захист основоположних прав і свобод фізичних осіб, зокрема їхнього права на захист персональних даних [8, ст. 1]. Регламент закріплює принципи обробки персональних даних (стаття 5), вимагає захисту даних за задумом і за замовчуванням (стаття 25), оцінки впливу на захист даних (стаття 35) і нагляду з боку органу, який діє з повною незалежністю (статті 51, 52) [8]. Для України як кандидата на членство в ЄС ці вимоги важливі передусім для самої держави, адже саме вона розпоряджається найбільшими масивами даних.

Найважливішим для цифрової держави я вважаю принцип обмеження мети [8, ст. 5]. Кожен реєстр створюється для конкретного завдання: реєстрації місця проживання, обліку платників податків, призначення соціальних виплат. Коли ж дані з різних реєстрів автоматично поєднуються, фактично з'являється нова мета обробки, якої людина не передбачала і яка потребує самостійної перевірки на відповідність законній меті обробки. Тож кожне нове поєднання даних, на мою думку, має спиратися на належну законну підставу та проходити оцінку необхідності й пропорційності.

Особливий режим діє в умовах воєнного стану. Частина друга статті 64 Конституції України дозволяє в умовах воєнного або надзвичайного стану встановлювати окремі обмеження прав і свобод із зазначенням строку дії цих обмежень, причому стаття 32 не входить до переліку статей, права за якими обмежувати не можна [1]. Право на захист персональних даних у цей період може обмежуватися, але не безмежно. І. Андронов та співавтори визнають допустимість таких обмежень в умовах воєнного стану, проте підкреслюють потребу визначити їх допустимі межі й передбачити механізми захисту права у випадках, коли втручання ці межі перевищує [5, с. 423, 430]. О. Тимошенко, своєю чергою, пов'язує актуальність проблеми з постійними кібератаками з боку держави-агресора і пропонує врегулювати особливі засоби захисту персональних даних у воєнний період спеціальним законом [4, с. 169, 170].

Оновити національне регулювання має проєкт Закону України «Про захист персональних даних» (реєстр. № 8153), який Верховна Рада України прийняла за основу 20 листопада 2024 року і який нині готується до другого читання [9]. Утім, сам по собі новий закон проблеми не розв'яже, якщо не з'явиться незалежний орган нагляду з реальними повноваженнями щодо органів

влади, а державні реєстри та «Дія» не підпадатимуть під ті самі вимоги, що й приватні компанії.

Наскільки ці питання практичні, добре видно на прикладі самої «Дії». У жовтні 2025 року Міністерство цифрової трансформації повідомило про урядове рішення щодо підсистеми моніторингу доступу до даних у системі «Трембіта» та запланованого інформування громадян через «Дію» про звернення органів влади до їхніх даних. Саме повідомлення не засвідчує повноцінного запуску такого функціоналу [10]. Винятки стосуються розслідування злочинів, контррозвідки, боротьби з тероризмом і досудового розслідування [10]. У перспективі, після впровадження відповідного функціоналу, особа зможе дізнаватися про звернення державних органів до її відомостей та перевіряти правомірність такого доступу. Як на мене, це вдалий приклад того, як право, закріплене у статті 8 Закону № 2297-VI [3], отримує технічне втілення.

Проте в цього механізму є слабе місце, його запроваджено постановою Кабінету Міністрів, а не законом, і перелік винятків теж визначає Уряд. Згідно з пунктом 1 частини першої статті 92 Конституції права і свободи людини і громадянина та гарантії цих прав і свобод визначаються виключно законами [1]. Тому вважаємо, що право знати про кожне звернення держави до своїх даних потрібно закріпити в законі. Для винятків варто передбачити відкладене повідомлення, після завершення розслідування людина має дізнатися, що її дані запитували.

Ширше кажучи, у цифровій державі гарантії статті 32 Конституції я розумію як позитивний обов'язок держави будувати свої інформаційні системи так, щоб захист даних був закладений у них від початку, а не додавався згодом.

Крім прозорості, про яку вже йшлося, такий підхід потребує ще трьох речей. Перша – законна підстава для кожного каналу обміну даними між реєстрами: з огляду на статтю 92 Конституції [1] обсяг міжреєстрової взаємодії, що зачіпає персональні дані, має визначатися законом, а не лише підзаконними актами. Друга – спеціалізований незалежний орган нагляду. Уповноважений Верховної Ради України з прав людини виконує дуже широке коло функцій, а контроль за обробкою даних державою в таких масштабах потребує окремої інституції з достатніми ресурсами, як того вимагають європейські стандарти [8, ст. 51, 52]. Третя – строковість обмежень. Розширена обробка даних, запроваджена у зв'язку з воєнним станом, з огляду на вимогу статті 64 Конституції про строк дії обмежень [1] і позицію ЄСПЛ щодо загального й невибіркового зберігання даних [7, п.125] має переглядатися після скасування воєнного стану.

Не можна оминати і безпековий бік проблеми, що більше даних зосереджено в державних системах, то тяжчими будуть наслідки витоку чи успішної кібератаки. Якщо держава зобов'язує людину передати свої дані до реєстру, вона бере на себе й обов'язок їх надійно захистити, а за порушення цього обов'язку має наставати реальна відповідальність, зокрема відшкодування шкоди.

Підсумовуючи, можна стверджувати, що конституційно-правові гарантії захисту персональних даних в Україні мають міцну основу. Стаття 32 Конституції, її тлумачення Конституційним Судом України, ратифікована Конвенція ETS № 108 та практика ЄСПЛ визнають обробку даних про особу без її згоди втручанням у приватне життя, допустимим лише на підставі закону, з легітимною метою та з дотриманням пропорційності. Зазначені гарантії не повною мірою пристосовані до цифрової держави, де саме держава є основним

розпорядником даних, а ризики виникають через масштаб, поєднання та тривале зберігання інформації.

З огляду на зазначене, пропонуємо:

1) завершити розгляд законопроекту № 8153 з поширенням його вимог на органи публічної влади в повному обсязі та одночасно створити незалежний орган нагляду у сфері захисту персональних даних;

2) закріпити обов'язкову оцінку впливу на захист даних перед запуском нових державних реєстрів і цифрових послуг, зокрема в «Дії»;

3) закріпити в законі право особи отримувати повідомлення про кожне звернення органів влади до її даних у державних реєстрах, механізм якого передбачено урядовим рішенням, і запровадити відкладене повідомлення для випадків, на які це право тимчасово не поширюється;

4) установити пропорційні строки зберігання персональних даних у державних реєстрах та забезпечити обов'язковий перегляд тимчасових обмежень після припинення або скасування воєнного стану.

Список використаних джерел

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96вр>

2. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12>

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>

4. Тимошенко О. А. Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. Аналітичнопорівняльне правознавство. 2023. № 4. С. 165–172. DOI: <https://doi.org/10.24144/2788-6018.2023.04.27>

5. Andronov I., Didenko L., Reznichenko S., Pozhodzhuk R., Romaniuk V. Limitations of the right to personal data protection and the right to secrecy of correspondence under martial law in Ukraine. Revista Jurídica Portucalense. 2024. No. 35. P. 423-438. DOI: [https://doi.org/10.34625/issn.2183-2705\(35\)2024.ic-20](https://doi.org/10.34625/issn.2183-2705(35)2024.ic-20)

10. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) : міжнар. док. від 28.01.1981 : ратифіковано Законом України від 06.07.2010 № 2438-VI. URL: https://zakon.rada.gov.ua/laws/show/994_326

11. S. and Marper v. the United Kingdom : judgment of the European Court of Human Rights (Grand Chamber) of 4 December 2008, applications nos. 30562/04 and 30566/04. URL: <https://hudoc.echr.coe.int/eng?i=001-90051>

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eurlex.europa.eu/eli/reg/2016/679/oj>

13. Про захист персональних даних : проєкт Закону України від 25.10.2022 № 8153. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707>

11. Українці зможуть бачити, хто і з якою метою переглядає їхні дані в реєстрах : повідомлення Міністерства цифрової трансформації України від 03.10.2025. Урядовий портал. URL:

<https://www.kmu.gov.ua/news/ukrainsizmozhut-bachyty-khto-i-ziakoiu-metoiu-perehliadaie-ikhni-dani-v-reiestrakh>

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

© Дарвай В.І., 2026

УДК 342.5:004.9(477)

КОНСТИТУЦІЙНО-ПРАВОВІ ЗАСАДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ

Зейкан Вероніка Василівна,
здобувачка другого (магістерського) рівня вищої освіти,
2-й курс, юридичний факультет,
Ужгородський університет,
м. Ужгород, Україна

Цифровізація публічного управління виступає ключовим вектором оновлення української правової системи, що охоплює не лише технічний вимір, а й фундаментальні інституційні та доктринальні засади [1, с. 128]. Йдеться не про просте переведення паперової документації в електронні формати, а про глибинну перебудову функціонування органів державної влади, якісну трансформацію процедурної логіки та переосмислення відносин між державою та громадянином. За таких умов цифровізація слугує рушієм системних перетворень у виконавчій гілці влади, сприяє міжвідомчій взаємодії та створює передумови для ухвалення управлінських рішень на основі аналізу великих масивів даних [1, с. 128].

Проблематика цифрової трансформації публічного управління протягом останніх років посідає чільне місце серед пріоритетів вітчизняної науки. Вагомий внесок у формування теоретичних підвалин цифровізації державного сектору зробили Н. Сорокіна, С. Квітка, В. Корсун та Ю. Магиляс, які розглядають діджиталізацію як вирішальний чинник модернізації системи державного управління й поетапного переходу до сервісно-орієнтованої моделі [4, с. 305]. У їхніх працях акцентовано увагу на реорганізації процесів надання публічних послуг, міжвідомчій інтеграції державних реєстрів та розбудові

цілісної екосистеми цифрових сервісів [4, с. 305], що безпосередньо впливає на прозорість, підзвітність та ефективність владних інститутів.

Важливий напрям наукового пошуку становлять дослідження М.Засухи, де підкреслюється значення цифрових платформ, алгоритмізації управлінських процесів та впровадження інструментів електронної демократії. Автором цифрова трансформація трактується як комплексний соціально-технологічний процес, що змінює не лише інструментарій, а й безпосередній зміст та логіку функціонування всієї державної системи.

Разом із тим, темпи технологічного розвитку зумовлюють постійну динаміку управлінських моделей, що вимагає подальшого глибокого юридичного осмислення [4, с. 305]. Перехід у цифровий формат передбачає всебічну модернізацію класичних інститутів адміністративного права. Насамперед змінюється сутність адміністративної процедури як унормованого порядку дій посадових осіб [1, с. 128]. Якщо традиційна система спиралася на персональний контакт та паперовий документообіг, то сучасна концепція базується на автоматизованій обробці відомостей, міжреєстровому обміні, засобах електронної ідентифікації та дистанційній комунікації. Відповідно, суттєвих змін зазнає і юридична природа управлінського рішення: поряд із класичними індивідуальними актами виникають рішення, згенеровані алгоритмічними системами [1, с. 128].

Оцифрування процесів змінює і формат взаємодії посадовців із населенням: від підходу «заява – очікування – відповідь» відбувається перехід до проактивного сервісу, коли надання послуги чи ініціювання розгляду здійснюється автоматично на основі аналітики держреєстрів [1, с. 129].

Цифрові інструменти також впливають на процедури контролю та притягнення до юридичної відповідальності [1, с. 129]. Завдяки логуванню дій

посадовців та фіксації цифрового сліду підвищується якість доказової бази під час перевірок або судових проваджень. Водночас постає потреба чіткого розмежування відповідальності між посадовою особою та автоматизованою системою у разі виникнення збоїв [1, с. 129].

Фундаментом цифрової трансформації громадянського залучення виступає зафіксована в Конституції України система фундаментальних суб'єктивних прав і засадничих принципів. Відповідно до статті 5 Конституції України, народ є носієм суверенітету та єдиним джерелом влади в Україні. Народ здійснює владу безпосередньо та через органи державної влади й органи місцевого самоврядування. В умовах цифрової трансформації реалізація цього конституційного принципу може доповнюватися цифровими формами участі громадян у публічному управлінні. Забезпечуючи це прагнення, ст. 38 стверджує фундаментальне право громадян брати участь в управлінні державними справами, яке за сучасних умов знаходить своє нове практичне втілення через цифрові канали та мережеві сервіси взаємодії з державою [5, ст. 5, ст.38].

Цей базис гармонійно доповнюється свободою висловлювання думок і вільним доступом до інформації (ст. 34), свободою об'єднання у громадські організації (ст. 36), а також правом на мирні зібрання (ст. 39), що сукупно формують сприятливе середовище для розгортання е-участі. Усі ці фундаментальні можливості мають імплементуватися в цифровому просторі через призму принципу рівності (ст. 24), що гарантує усунення бар'єрів та створення однакового доступу кожного громадянина до електронних інструментів [5, ст. 34, ст. 39, ст.36, ст.24].

Еволюція конституційних гарантій в умовах цифрової реальності диктує потребу в їх належному інституційному опосередкуванні через

взаємоузгоджену діяльність публічного сектору та інституцій громадянського суспільства. Становлення електронної демократії виходить за межі суто декларативного закріплення прав у законодавстві – воно вимагає злагодженої роботи конкретних суб'єктів, наділених відповідною компетенцією та сучасним цифровим інструментарієм. Саме тому систематизація ключових елементів інституційного механізму е-демократії в Україні дозволяє чітко окреслити його архітектурні особливості, розкрити наявні деструкції та визначити стратегічні вектори подальшої модернізації [2, с.11].

Повноцінне функціонування е-демократичних процесів неможливе без кардинального посилення адміністративно-правових важелів належного врядування – передусім у контексті впровадження ефективного контролю, підзвітності та прозорості суб'єктів владних повноважень. Власне, органам публічної влади належить стрижнева роль у цьому процесі: вони формують регуляторну базу, забезпечують технологічну інфраструктуру та контролюють практичне втілення цифрових сервісів. Поряд із цим реальна ефективність електронного народовладдя виникає лише за умови рівноправного партнерства держави з інститутами громадянського суспільства, які виступають рушійною силою – ініціюють, наповнюють змістом та здійснюють громадський контроль за е-участю. Тільки за такої взаємодії цифрове врядування стає справді відкритим, підзвітним і орієнтованим на задоволення реальних запитів суспільства [2, с.11].

На мою думку, цифровізація публічної влади в Україні потребує чітких конституційних меж і повинна спиратися на кілька принципових положень. Насамперед технології не мають обмежувати права людей. Популярний підхід цифровізація за замовчуванням є зручним, проте держава зобов'язана зберігати й класичні паперові чи очні процедури. Якщо людина не має смартфона,

доступу до мережі чи відповідних навичок, вона не повинна втрачати можливість отримувати державні послуги, адже протилежне прямо порушує принцип рівності прав, закладений у статті 24 Конституції України.

Крім того, алгоритми не можуть ухвалювати складні управлінські рішення. Повністю автоматичні системи без участі чиновника допустимі лише там, де немає місця для оцінки чи суб'єктивного вибору, як-от у стандартній реєстрації чи розрахунку виплат за чіткою математичною формулою. Якщо розгляд справи потребує оцінювання індивідуальних обставин, застосування адміністративного розсуду або врахування інших юридично значущих чинників, використання автоматизованих систем має здійснюватися з дотриманням установлених законом процедурних гарантій. Доцільно передбачити належний людський контроль за такими рішеннями, а також можливість їх перевірки та оскарження у встановленому законом порядку [2, с.12].

Разом із цим важливо забезпечити право людини знати, як саме спрацював алгоритм. У разі відмови в наданні публічної послуги або виплати особі має бути забезпечена можливість отримати належне обґрунтування прийнятого адміністративного акта, зокрема відомості про фактичні та правові підстави рішення, а також інформацію про порядок і строки його адміністративного та судового оскарження. Якщо рішення ухвалено із застосуванням автоматизованої системи, доцільно передбачити можливість отримання пояснення щодо істотних чинників, які вплинули на результат.

Одним із можливих напрямів удосконалення законодавства є розроблення та прийняття спеціального нормативно-правового акта, який визначатиме вимоги до прозорості алгоритмічних систем у публічному секторі, порядок

оцінювання їхніх ризиків, механізми людського контролю та гарантії захисту прав осіб, на яких впливають автоматизовані рішення.

Поряд із цим вагомої адаптації до умов цифрової трансформації суспільних відносин потребує Закон України «Про адміністративну процедуру». Комплексне вдосконалення цього акта передбачає нормативно-правове розширення окремого блоку щодо електронних проваджень, деталізацію правил використання системних записів і лог-файлів як належних та допустимих доказів у справі, а також оновлення законодавства про захист персональних даних відповідно до стандартів Європейського Союзу задля запобігання безконтрольному міжвідомчому обміну інформацією. Особливої уваги в цьому контексті потребує стаття 69 Закону («Прийняття рішення у справі»), частина друга якої наразі лише загально передбачає можливість ухвалення адміністративного акта в автоматичному режимі у випадках, зафіксованих законом, за умови використання електронних документів у машинозчитувальному форматі чи даних національних електронних інформаційних ресурсів[3, ст. 69]. З метою підвищення рівня правової визначеності та посилення гарантій захисту прав особи доцільно розглянути можливість удосконалення законодавчого регулювання автоматичного прийняття адміністративних актів, зокрема шляхом конкретизації вимог до мотивування таких актів, інформування особи про застосування автоматизованої системи та забезпечення ефективних механізмів їх перегляду й оскарження.

У сфері судової практики Верховний Суд має сформулювати чітку позицію щодо технічних збоїв. У разі технічного збою електронної системи або передавання некоректних даних необхідно забезпечити механізми встановлення причин збою, виправлення його наслідків та захисту прав особи. Питання

юридичної відповідальності відповідного органу публічної влади або конкретних посадових осіб має вирішуватися з урахуванням характеру порушення, наявності передбачених законом підстав і причинного зв'язку між відповідними діями чи бездіяльністю та завданою шкодою.

Перехід у цифровий формат виступає не просто відмовою від паперового документообігу, а глибинною зміною всієї логіки функціонування держави. Вона докорінно трансформує порядок збирання доказів, перевірки юридичних фактів та комунікації між посадовцями й населенням [1, с. 130; 4, с. 305]. Водночас основними ризиками цифровізації на цьому етапі залишаються загрози витоку персональних даних, цифровий розрив між різними верствами населення, а також ризик ухвалення некоректних рішень автоматизованими системами, за які складно притягнути до відповідальності конкретну посадову особу [1, с. 132]. Ключовим правилом цифрової держави має залишатися те, що будь-які технології покликані спрощувати життя людині та захищати її права, а не ставати інструментом надмірного контролю чи нових бюрократичних перешкод. Усі електронні процедури мають залишатися прозорими, зрозумілими та повністю підконтрольними людині.

Список використаних джерел

1. Дубіна Є. Е., Лютіков П. С. Правові засади цифрової трансформації публічного адміністрування в Україні: доктринальні та нормопроєктні аспекти. Нове українське право. 2026. Вип. 1. С. 127–133. URL: https://www.researchgate.net/publication/404665782_PRAVOVI_ZASADI_CIFROVOI_TRANSFORMACII_PUBLICNOGO_ADMINISTRUVANNA_V_UKRAINI_DOKTRINALNI_TA_NORMOPROEKTNI_ASPEKTI (дата звернення: 11.10.2026).

2. Захарчин Н. Г., Пугач Д. О., Плугатар Т. А. Електронна демократія та конституційні гарантії участі громадян в умовах європейської інтеграції України. *Український політико-правовий дискурс*. 2026. С. 1–18. URL: <https://doi.org/10.5281/zenodo.20441740> (дата звернення: 15.10.2026).
3. Про адміністративну процедуру : Закон України від 17 лют. 2022 р. № 2073-IX. *Відомості Верховної Ради України*. 2023. № 15. Ст. 50. URL: <https://zakon.rada.gov.ua/laws/show/2073-20#n517> (дата звернення: 15.10.2026).
4. Тюріна Д. М., Карпеко Н. М., Балабушкін К. С. Нормативно-правові засади цифрової трансформації публічного управління в Україні. *Інвестиції: практика та досвід*. 2025. № 24. С. 303–308. URL: <https://www.nayka.com.ua/index.php/investplan/article/view/8439/8577> (дата звернення: 11.10.2026).
5. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 15.10.2026).

Дата першого надходження рукопису до видання: 16.10.2026

Дата прийняття до друку рукопису після рецензування: 21.10.2026

Дата публікації: 27.10.2026

УДК 342.7:004(477)

ЦИФРОВІ ПРАВА ЛЮДИНИ У СИСТЕМІ СУЧАСНОГО КОНСТИТУЦІОНАЛІЗМУ

Лендьял Анастасія Василівна,
студентка 2-го курсу магістратури
юридичного факультету
Ужгородський університет

Використання сучасних цифрових технологій обумовило головні етапи перетворень в сучасному суспільстві – цифрову трансформацію суспільних відносин, яка обумовлена в застосуванні сучасних цифрових технологій в різноманітних сферах діяльності людини. Цифрова революція як фактор динамічного розвитку привела до створення цифрової економіки, формування засад цифрового права, нової конфігурації соціальних відносин на базі використання мережі Інтернет, соціальних мереж, інших інформаційно-комунікаційних технологій. Сучасні цифрові технології формують новий спосіб виробництва, створюють передумови для переходу до нової формації, до цифровізації суспільних відносин і самого права, що регулює ці відносини. Цифрова трансформація здійснює безпосередній вплив на реалізацію фундаментальних прав людини, сприяє появі нових прав людини і громадянина як учасника глобального інформаційного та цифрового простору. Результати цифровізації вимагають осмислення та адекватного формулювання правового механізму регулювання, реалізації та захисту вже існуючих та тих, які тільки на початку формування, прав людини з метою сталого соціально-економічного розвитку, забезпечення реалізації конституційних прав і свобод людини і громадянина.

Цифрові права доцільно розглядати як інтегративний сегмент системи прав людини, що поєднує інформаційний, технологічний та соціальний виміри. Цифровізація суспільства впливає не лише на зміст прав людини, а й на саму природу конституціоналізму. У сучасному науковому дискурсі формується концепція цифрового конституціоналізму, що спрямована на адаптацію фундаментальних принципів верховенства права, демократії та поділу влади до умов цифрового суспільства. Права людини історично формувалися як відповідь на соціальні конфлікти, технологічні зміни та трансформацію влади. Кожна епоха розширювала розуміння людської гідності як фундаментальної конституційної цінності. У цифрову добу змінюється не лише форма реалізації прав, а й сама структура соціальної взаємодії. Цифрові технології створюють новий простір існування людини – цифрову публічну сферу. Якщо раніше держава була основним суб'єктом потенційного втручання у права людини, то сьогодні значну частину владних повноважень реалізують приватні цифрові корпорації. У цьому контексті особливої ваги набуває принцип людської гідності як мета-норма конституційного порядку. Цифрові права повинні розглядатися як продовження і конкретизація гарантій людської гідності в умовах алгоритмічного середовища. Принцип верховенства права є основою сучасного конституціоналізму. Втручання у сферу приватності можливе лише за наявності чітких, передбачуваних і пропорційних правових підстав. У цифровому середовищі принцип верховенства права стикається з новими викликами: непрозорість алгоритмів, автоматизоване прийняття рішень, масове збирання персональних даних, складність юрисдикційного контролю над транснаціональними платформами. [1, с.196].

Як стверджують Петришин О. В. та Гиляка О. С. сфера цифрових відносин характерна ознаками віртуальності та транскордонності, потребує

особливої уваги до сфери основних прав людини з точки зору їх забезпечення з урахуванням особливих властивостей цього середовища, де суб'єкти та об'єкти дуже часто виступають своєрідною «симуляцією», а межі здійснення прав індивідів і втручання в них не завжди однозначно ідентифікуються. Як показує практика розвитку права в сучасному світі, в понятійно-правовий обіг поступово вводиться категорія «цифрові права» (які ще іменують, як інтернет-права, мережеві права), що набула поширення, як вагомий елемент для характеристики правового стану особи в мережі Інтернет. У той же час така категорія прав, як «цифрові права», до теперішнього часу не отримала загального визнання ні в праві, ні в доктрині, в тому числі з огляду на вітчизняний правовий та правозастосовний досвід. Очевидно, це пов'язано з тим, що проблема пошуку, визначення специфіки основних прав людини (їх змісту та реалізації) в цифровому середовищі виникла порівняно недавно і, можливо, вирішення цього питання – справа найближчого майбутнього [2, с.19].

Варто відзначити, що процес цифровізації визначає стирання меж між основоположними галузями права. Інформація та технології вже наявні в кожній галузі, вони є спільним знаменником і спроможні визначати однакову логіку права. Важливість меж галузей права знижується в правовій практиці, що неминуче має вплив й на теорію права. Категорія цифрових прав одержує поетапне визнання в глобальному, регіональному і національному значенні. Іноді це здійснюється в порядку визначення конкретних прав людини, які варто відносити до цифрових, комунікаційних, іноді ж на значно загальній основі – при обґрунтуванні детального переліку таких прав.

Щерба О.С., Ухаль К.П. та Продан В.І. вважають, що серед ключових проблем правового забезпечення цифрових прав в Україні передусім слід виокремити фрагментарність нормативного регулювання та відсутність

цілісного законодавчого підходу до визначення їх змісту і гарантій реалізації. Така розпорошеність правового регулювання, що проявляється у наявності численних норм у нормативно-правових актах різної юридичної сили без належного системного узгодження, зумовлює складність правозастосування як на національному, так і на міжнародному рівнях. Водночас відсутність уніфікованої правової категорії «цифрові права» та спеціального законодавчого акта, який би комплексно закріплював їх перелік і механізми захисту, призводить до їх галузевої роздробленості, попри усталене доктринальне сприйняття цифрових прав як окремої групи прав людини, сформованої під впливом цифровізації суспільних відносин. Окремої уваги заслуговує також проблема недостатньої ефективності правозастосування, що виявляється у відсутності усталеної судової практики та єдиних правових позицій, складності збирання і фіксації цифрових доказів, особливо у випадках транскордонного зберігання інформації, а також у недосконалості процедур притягнення до юридичної відповідальності за порушення цифрових прав. У сукупності ці чинники свідчать про те, що, попри поступове формування нормативної та інституційної бази, фактична реалізація цифрових прав в Україні залишається обмеженою та потребує системного вдосконалення, зокрема шляхом кодифікації відповідних норм, гармонізації з правом Європейського Союзу та розвитку ефективних механізмів їх гарантування і захисту [3, с.545].

Проблема пошуку, визначення специфіки основних прав людини (їх змісту та реалізації) в цифровому середовищі утворилася порівняно недавно і, можливо, вирішення даного питання – справа найближчого майбутнього. В загальному понятті під цифровими правами варто розуміти розширення універсальних прав особи до потреб суспільства, визначеного на інформації. Вважаємо, що цифрові права мають включати обширне коло основоположних

прав, які здійснюються в цифровому середовищі і потребують ґрунтовного аналізу з точки зору особливостей цього середовища. При цьому основні цифрові права вважаються перш за все похідними від інформаційних прав, але до них не відносяться.

Вважається, що тенденції управління технічною інфраструктурою щодо напрямку її фрагментації, поляризації та гібридизації, сприяють змінам архітектури свободи й влади в цифровому середовищі, надаючи відповідний поштовх для нової ролі конституціоналізму. Тому, як стверджує Бесчастний В., ключова наукова дискусія точиться навколо питання, наскільки новації в регулюванні мережею Інтернет призведуть до створення нової конституційної парадигми в епоху цифрових технологій [4, с.11].

На думку Захарчука І.В., рівень цифрової безпеки в Україні залишається недостатнім, особливо в умовах зростання масштабів кібератак, пов'язаних з воєнним станом та агресією РФ. Найпоширеніші технічні виклики це кібератаки на державні реєстри та критичну інфраструктуру (наприклад, атаки на «Дію» та інші державні сервіси), використання шкідливого програмного забезпечення для збору персональних даних громадян, а також недостатній рівень захисту каналів передачі інформації, особливо у сфері електронного документообігу [5, с.271].

Отже, цифрові права повинні забезпечувати: юридичну визначеність алгоритмічних рішень; можливість оскарження автоматизованих процедур; прозорість обробки персональних даних; ефективні механізми судового захисту. Цифровізація державного управління призводить до використання автоматизованих систем у сферах соціального забезпечення, податкового адміністрування, правопорядку. Європейський суд з прав людини у своїй практиці послідовно підкреслює, що обмеження свободи слова повинні бути

пропорційними та необхідними в демократичному суспільстві. Водночас цифрові платформи встановлюють власні правила спільнот, що фактично виконують регуляторну функцію. Таким чином, цифрові права набувають рис соціальних прав, що потребують позитивних зобов'язань держави. В Україні інфраструктура правової охорони та захисту цифрових прав формується в контексті євроінтеграційних зусиль. Правові системи сучасності постали перед фундаментальним викликом – докорінною зміною технологічної парадигми, що виявляє себе у формуванні інфраструктури цифрового світу. Було з'ясовано, що цифровізація вже пронизує собою все людське життя, впливаючи на самовизначення людини, її комунікацію з іншими, форми соціалізації та багато іншого. Масштабування й тотальність цифрових сервісів, платформ, інструментів сягає самого ціннісного і смислового ядра європейської цивілізації – основоположних прав людини. Основоположні права людини повинні зберігати велике аксіологічне значення й в умовах цифрового світу. Правосуддя набуває першочергового значення для цифровізації традиційних прав людини, надання їм нових цифрових конотацій. Цифрові права – це нова форма вираження традиційних прав людини. При цьому ця нова форма вимагає нового налаштування балансу між свободою вираження, безпекою та приватністю. Алгоритмічне врядування потребує нових гарантій прозорості та підзвітності. Україна перебуває на етапі активного формування системи конституційних гарантій цифрових прав у контексті євроінтеграції. Остання й визначає стратегічний напрям розвитку цифрових прав в Україні. Цифрові права є невід'ємною складовою сучасного конституційного правопорядку.

Список використаних джерел

1. Сапарова А. О. Цифрові права людини в системі конституційних цінностей: теоретико-правові засади. *Аналітично-порівняльне правознавство*. 2026. № 2. Ч. 1. С. 193–198. DOI: <https://doi.org/10.24144/2788-6018.2026.02.1.28>. URL: <https://app-journal.in.ua/wp-content/uploads/2026/04/30.pdf> (дата звернення: 15.10.2026).
2. Петришин О. В., Гиляка О. С. Права людини у цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. Т. 28. № 1. С. 7–35. DOI: <https://doi.org/10.31359/1993-0909-2021-28-1-17>. URL: https://ccu.gov.ua/sites/default/files/petryshyn_o._v._gylyaka_o._s._prava_lyudyny_v_cyfrovu_epohu.pdf (дата звернення: 16.10.2026).
3. Щерба О. С., Ухаль К. П., Продан В. І. Проблематика нормативної ідентифікації цифрових прав людини в системі конституційних прав. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Вип. 94. Ч. 2. С. 542–546. DOI: <https://doi.org/10.24144/2307-3322.2026.94.2.79>. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2026/05/81.pdf> (дата звернення: 15.10.2026).
4. Бесчастний В. М., Костицький М. В., Кушакова-Костицька Н. В. Цифровий конституціоналізм: нова парадигма та перспективи розвитку в Україні. *Філософські та методологічні проблеми права*. 2022. Т. 24. № 2. С. 9–26. DOI: <https://doi.org/10.33270/02222402.9>. URL: <https://philosophy.navs.edu.ua/index.php/philosophy/article/view/1510> (дата звернення: 14.10.2026).
5. Захарчук І. В. Цифрові права громадян України: конституційно-правове закріплення та механізми реалізації. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90. Ч. 1. С. 268–273. DOI:

<https://doi.org/10.24144/2307-3322.2025.90.1.34>.

URL:

<https://visnyk-pravo.uzhnu.edu.ua/article/view/340322/328321> (дата звернення: 15.10.2026).

Дата першого надходження рукопису до видання: 16.10.2026

Дата прийняття до друку рукопису після рецензування: 21.10.2026

Дата публікації: 27.10.2026

© Лендъел А.В., 2026

УДК 342.727:004.738.5(477)

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ У СОЦІАЛЬНИХ МЕРЕЖАХ: СПІВВІДНОШЕННЯ ПРИВАТНОЇ МОДЕРАЦІЇ ТА КОНСТИТУЦІЙНИХ ГАРАНТІЙ

Луканич Ярослава Іванівна,
магістр, спец. право, 2 курс, заочн. ф.н.,
Ужгородський університет

Сьогодні люди спілкуються і висловлюють свою думку здебільшого в соціальних мережах. Але ці мережі належать приватним компаніям, які самі вирішують, який контент видаляти, а які акаунти блокувати, керуючись власними правилами користування. При цьому Конституція України у ст. 34 [1] та Конвенція про захист прав людини і основоположних свобод у ст. 10 [2] гарантують кожному свободу вираження поглядів. Виникає протиріччя: держава зобов'язана захищати свободу слова, а приватні компанії, які фактично контролюють головний простір спілкування, формально не є суб'єктами публічної влади і конституційними нормами не зв'язані. Через це виникає ризик прихованої цензури з боку самих платформ, яку державі складно контролювати.

У науці конституційного права вже давно обговорюють ідею про те, що конституційні права можуть діяти не лише у відносинах людини з державою, а й у відносинах між приватними особами (так звана горизонтальна дія прав). Але щодо соціальних мереж ця ідея почала активно досліджуватися лише останніми роками. Європейський суд з прав людини у справі *Delfi AS* проти Естонії (заява № 64569/09, рішення від 16 червня 2015 р.) визнав, що держава повинна дбати про реальне здійснення свободи вираження поглядів, навіть коли йдеться про приватну інтернет-платформу [3]. Європейський Союз пішов далі й ухвалив Регламент (ЄС) 2022/2065 про цифрові послуги (Digital Services Act)

від 19 жовтня 2022 р. [4]. Він зобов'язує платформи пояснювати причини видалення контенту, дає користувачам право оскаржити таке рішення і вимагає прозорості в роботі алгоритмів. В Україні подібного закону поки немає: чинне законодавство про медіа регулює діяльність соціальних мереж лише частково, а стала практика Конституційного Суду України з цього питання ще не сформувалася.

На нашу думку, те, що соціальні мережі є приватними компаніями, не означає, що вони можуть повністю ігнорувати конституційні гарантії свободи слова. Є три причини так вважати. По-перше, кілька великих компаній фактично монополізували простір, де відбувається публічне спілкування. По-друге, у користувача часто немає реальної альтернативи. По-третє, при укладенні договору користування (коли людина погоджується з правилами платформи) сторони явно нерівні, оскільки платформа диктує умови, а користувач може лише погодитися або відмовитися від сервісу повністю. Тому вважаємо правильним дотримання принципу, за яким держава не поширює конституційні норми на приватні платформи напряму, а натомість зобов'язує їх через звичайні закони дотримуватися певних гарантій, а саме: пояснювати причини видалення контенту чи блокування, давати можливість оскаржити таке рішення, не допускати модерації через політичні чи релігійні погляди користувача, а також розкривати принципи роботи рекомендаційних алгоритмів.

Проведене дослідження дає підстави констатувати, що забезпечення свободи вираження поглядів у соціальних мережах набуває особливого конституційно-правового значення з огляду на посилення впливу приватних цифрових платформ на реалізацію інформаційних прав людини. Незважаючи на те, що конституційні гарантії свободи вираження поглядів насамперед визначають межі допустимого втручання держави, їх реалізація в цифровому

середовищі потребує належного нормативного врегулювання відносин між користувачами та адміністраторами соціальних мереж. У цьому контексті особливого значення набувають позитивні зобов'язання держави щодо формування правових механізмів, здатних запобігати свавільному обмеженню свободи вираження поглядів приватними суб'єктами.

Перспективним напрямом удосконалення національного законодавства вбачається запровадження правових стандартів модерації цифрового контенту з урахуванням положень Регламенту (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг (Digital Services Act). Пріоритетного значення потребує нормативне закріплення обов'язку цифрових платформ надавати користувачам належне обґрунтування рішень щодо видалення контенту, обмеження його поширення, блокування облікових записів та застосування інших заходів модерації. Необхідною гарантією захисту свободи вираження поглядів має стати забезпечення доступних, прозорих та ефективних процедур оскарження відповідних рішень, які унеможливлювали б необґрунтоване втручання у здійснення інформаційних прав користувачів.

Слід підкреслити, що уваги заслуговує також питання інституційного забезпечення захисту прав користувачів соціальних мереж. У зв'язку із цим доцільним видається опрацювання можливості запровадження незалежного механізму позасудового розгляду спорів у сфері модерації цифрового контенту, зокрема шляхом створення спеціалізованої інституції медіаомбудсмена або наділення відповідними повноваженнями незалежного органу з належними гарантіями інституційної автономії.

Список використаних джерел

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 23.09.2026).
2. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/995_004 (дата звернення: 23.09.2026).
3. Case of Delfi AS v. Estonia, Application no. 64569/09, Grand Chamber, ECtHR, judgment of 16 June 2015. URL: <https://hudoc.echr.coe.int> (дата звернення: 23.09.2026).
4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022, p. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (дата звернення: 23.09.2026).

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.8

ЦИФРОВИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ ЯК КАТЕГОРІЯ СУЧАСНОГО КОНСТИТУЦІЙНОГО ПРАВА

Марковцїй Крістіна,

здобувачка другого (магістерського) рівня вищої освіти
спеціальності D8 «Право»

ДВНЗ «Ужгородський національний університет»

ORCID: <https://orcid.org/0009-0000-4368-0227>

Розвиток цифрових технологій істотно змінює характер взаємодії між державою, суспільством і людиною. Електронне урядування, цифрові реєстри, хмарні обчислення, штучний інтелект та транскордонний обмін даними вже стали невіддільними складовими публічного управління. Водночас ці процеси порушують питання про межі державної влади в цифровому середовищі, можливості захисту національних інформаційних ресурсів і забезпечення конституційних прав людини.

Традиційне розуміння державного суверенітету ґрунтується на верховенстві державної влади всередині країни та її незалежності в міжнародних відносинах. Однак у сучасних умовах реальна спроможність держави здійснювати свої повноваження дедалі більше залежить від доступу до цифрової інфраструктури, контролю над державними даними, захищеності інформаційних систем і здатності протидіяти зовнішньому технологічному впливу. У зв'язку з цим виникає потреба дослідити цифровий суверенітет не лише як напрям державної політики, а і як категорію сучасного конституційного права.

Наукова актуальність цієї проблематики полягає в тому, що цифровий суверенітет не має єдиного загальновизнаного визначення. У дослідженні Ю.

Поле та Т. Тіля наголошено на дискусійності цього поняття та різноманітності його політичних і нормативних інтерпретацій [1]. У свою чергу, Г. Робертс та співавтори аналізують цифровий суверенітет у контексті захисту європейських цінностей, управління даними, регулювання цифрових платформ, розвитку інфраструктури та кібербезпеки [2]. Ці дослідження свідчать про необхідність комплексного підходу до визначення правової природи цифрового суверенітету.

Для України зазначена проблема має особливе значення. В умовах збройної агресії та постійних кіберзагроз забезпечення безперервності роботи державних інформаційних систем, захисту електронних реєстрів і стійкості критичної інфраструктури безпосередньо пов'язане з реалізацією функцій держави. Водночас посилення цифрової безпеки не повинно призводити до необґрунтованого обмеження свободи слова, порушення приватності чи надмірної концентрації інформаційних повноважень у руках державних органів.

Метою роботи є визначення змісту цифрового суверенітету держави як категорії сучасного конституційного права, з'ясування його нормативних засад, дослідження співвідношення з основоположними правами людини та обґрунтування напрямів удосконалення законодавства України.

Цифровий суверенітет є відносно новою категорією, зміст якої формується під впливом технологічних, політичних, економічних і правових змін. Його виникнення пов'язане з тим, що традиційні механізми здійснення державної влади дедалі частіше залежать від цифрових систем, які можуть перебувати під контролем приватних компаній або функціонувати в межах інших юрисдикцій.

Ю. Поле та Т. Тіль звертають увагу на те, що цифровий суверенітет використовується в різних політичних контекстах, а його зміст не обмежується питаннями державного контролю над інтернетом. Він також охоплює проблеми

самовизначення, управління технологіями та визначення правил функціонування цифрового середовища [1]. Вказане дає підстави стверджувати, що цифровий суверенітет не можна зводити виключно до технологічної незалежності або контролю над інформаційними потоками. У контексті конституційного права важливим є визначення зв'язку цифрового суверенітету з основоположними принципами організації державної влади. Відповідно до статті 1 Конституції України, Україна є суверенною і незалежною, демократичною, соціальною, правовою державою. Згідно зі статтею 5, носієм суверенітету та єдиним джерелом влади в Україні є народ. Стаття 19 Основного Закону закріплює принцип законності діяльності органів державної влади, а статті 32 і 34 гарантують відповідно право на невтручання в особисте і сімейне життя та свободу думки і слова [3]. Зазначені положення не містять окремого визначення цифрового суверенітету, проте створюють конституційну основу для його осмислення. Зокрема, народний суверенітет передбачає, що цифрові інструменти публічного управління повинні сприяти реалізації волі народу, а не підміняти її непрозорими алгоритмами або неконтрольованими механізмами прийняття рішень. Принцип законності, своєю чергою, означає, що використання державою цифрових технологій має здійснюватися в межах установлених повноважень і за наявності належної правової підстави.

На нашу думку, цифровий суверенітет держави доцільно визначати як засновану на Конституції та законах України спроможність держави самостійно визначати правові засади функціонування цифрового середовища, забезпечувати стійкість критичної цифрової інфраструктури, захищати інформаційні ресурси та здійснювати публічну владу із дотриманням прав і свобод людини. Таке визначення має кілька принципових особливостей. По-перше, воно пов'язує цифровий суверенітет із правовою природою

державної влади. По-друге, передбачає не абсолютну технологічну автономію, а реальну спроможність управляти цифровими ризиками. По-третє, встановлює права людини як обов'язкову межу здійснення державних повноважень у цифровому середовищі.

Відтак, цифровий суверенітет слід розглядати як функціональний вимір державного суверенітету, який набуває особливого значення в умовах цифровізації суспільних відносин.

Правове регулювання цифрового середовища в Україні здійснюється за допомогою низки нормативно-правових актів, які регулюють інформаційні відносини, кібербезпеку, захист персональних даних та функціонування електронних реєстрів. Одним із ключових актів у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Він визначає правові й організаційні основи забезпечення захисту національних інтересів України в кіберпросторі, а також установлює засади діяльності відповідних суб'єктів у сфері кібербезпеки [4]. Значення цього Закону для цифрового суверенітету полягає в тому, що захищеність державних інформаційних ресурсів та інформаційно-комунікаційних систем є необхідною умовою належного здійснення публічної влади. Водночас кібербезпека становить лише один зі складників цифрового суверенітету. Важливе значення має також Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, який визначає правові засади обробки персональних даних та спрямований на захист основоположних прав і свобод людини у зв'язку з такою обробкою [5]. У цифровому середовищі персональні дані набувають особливого значення, оскільки можуть накопичуватися в державних реєстрах, інформаційних системах приватних компаній та автоматизованих платформах. Неналежне використання таких даних створює

ризиками для приватності, особистої автономії та свободи людини. Тому спроможність держави контролювати законність обробки інформації має розглядатися не тільки як елемент інформаційної політики, а й як гарантія конституційних прав. Окрему роль відіграє Закон України «Про публічні електронні реєстри» від 18 листопада 2021 року № 1907-IX, який установлює правові засади створення, функціонування та взаємодії публічних електронних реєстрів [6].

Належна організація таких реєстрів є важливою для забезпечення достовірності державних даних, доступності адміністративних послуг і безперервності роботи органів публічної влади. Проте наявність відповідних законодавчих актів не означає, що всі питання цифрового суверенітету вже врегульовані. Чинне законодавство регулює переважно окремі напрями цифрових відносин, тоді як комплексні критерії технологічної стійкості, управління критичними цифровими залежностями та співвідношення державного контролю із правами людини потребують подальшого системного осмислення.

Важливим орієнтиром для такого осмислення є Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012, ухвалене у справі щодо офіційного тлумачення положень частин першої та другої статті 32, а також частин другої та третьої статті 34 Конституції України [7]. У цьому рішенні Суд розкрив зміст інформації про особисте та сімейне життя людини, наголосивши на необхідності врахування конституційних гарантій приватності під час збирання, зберігання, використання та поширення інформації. Для сучасних цифрових відносин це рішення має особливу вагу. Автоматизована обробка інформації, взаємодія державних реєстрів та використання алгоритмічних систем збільшують можливості накопичення відомостей про особу. Відповідно,

цифровий розвиток держави повинен супроводжуватися належними гарантіями конфіденційності, законності обробки даних та ефективного захисту прав людини.

Таким чином, нормативна база України створює передумови для реалізації цифрового суверенітету, але потребує подальшого розвитку в напрямі комплексного узгодження питань національної безпеки, цифрової інфраструктури, управління даними та конституційних гарантій.

Значний інтерес для дослідження цифрового суверенітету становить досвід Європейського Союзу. У науковій статті Г. Робертса, Дж. Коулза, Ф. Казоларі, Дж. Морлі, М. Таддео та Л. Флоріді досліджено, як європейські інституції пов'язують цифровий суверенітет із захистом європейських цінностей, управлінням даними, регулюванням цифрових платформ і розвитком інфраструктури [2]. Автори показують, що досягнення цифрової незалежності залежить не лише від технологічних ресурсів, а й від спроможності встановлювати ефективні правила для державних та приватних суб'єктів. Одним із основних нормативних актів ЄС у сфері захисту інформації є Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року - Загальний регламент про захист даних (GDPR) [8]. Він установлює правила захисту фізичних осіб у зв'язку з обробкою персональних даних та їх вільним рухом. Значення цього документа полягає в тому, що захист персональних даних розглядається як системна правова вимога, яка поширюється на відповідні процеси обробки інформації. Іншим важливим документом є Регламент (ЄС) 2022/868 від 30 травня 2022 року про європейське управління даними (Data Governance Act) [9], котрий спрямований на формування правових механізмів управління даними та сприяння їх доступності й повторному використанню за встановлених умов. У контексті

цифрового суверенітету це свідчить про важливість належних процедур управління даними, які дають змогу поєднувати їх практичну цінність із дотриманням правових обмежень. Особливого значення в умовах розвитку штучного інтелекту набуває Регламент (ЄС) 2024/1689 від 13 червня 2024 року, відомий як Акт про штучний інтелект (AI Act) [10]. Документ установлює гармонізовані правила щодо штучного інтелекту та використовує ризик-орієнтований підхід до регулювання відповідних систем. Для конституційного права цей підхід важливий тому, що застосування алгоритмів у публічному управлінні може впливати на реалізацію прав людини, доступ до адміністративних послуг і характер взаємодії особи з державою.

Зазначені регламенти ЄС не слід автоматично вважати безпосередньо обов'язковими для України в повному обсязі. Їхнє значення для українського правопорядку визначається, зокрема, міжнародними зобов'язаннями України, сферою застосування відповідних актів і процесом наближення національного законодавства до права ЄС. Водночас вони є важливими нормативними орієнтирами для вдосконалення українського законодавства.

Не менш важливою є практика Європейського суду з прав людини. У справі *Big Brother Watch and Others v. the United Kingdom* Велика палата ЄСПЛ 25 травня 2021 року розглянула питання масового перехоплення комунікацій, отримання комунікаційних даних від постачальників послуг та обміну розвідувальною інформацією [11]. Суд установив порушення статті 8 Конвенції щодо режиму масового перехоплення комунікацій і режиму отримання комунікаційних даних від постачальників послуг, а також порушення статті 10 у відповідних аспектах, пов'язаних із недостатніми гарантіями захисту журналістських матеріалів.

Виходячи з наведеного, використання державою сучасних технологій спостереження має супроводжуватися належними правовими гарантіями. Навіть якщо відповідні заходи переслідують легітимну мету захисту національної безпеки, вони повинні відповідати вимогам законності та забезпечувати належний захист від свавільного втручання у приватне життя і свободу вираження поглядів. Важливим міжнародним документом є також Рамкова конвенція Ради Європи про штучний інтелект і права людини, демократію та верховенство права (CETS № 225), відкрита для підписання 5 вересня 2024 року [12]. Конвенція спрямована на забезпечення відповідності діяльності протягом життєвого циклу систем штучного інтелекту принципам прав людини, демократії та верховенства права. Її значення полягає у формуванні міжнародного підходу, за якого розвиток штучного інтелекту має супроводжуватися належними правовими гарантіями. Так, європейські стандарти підтверджують, що цифровий суверенітет не може розглядатися окремо від захисту основоположних прав людини. Ефективність державної цифрової політики залежить не тільки від технічної захищеності інформаційних систем, а й від наявності чітких правил, незалежного контролю та доступних засобів правового захисту.

На нашу думку, цифровий суверенітет держави повинен розглядатися як комплексна конституційно-правова категорія, що поєднує державну спроможність, технологічну стійкість і гарантії прав людини. Такий підхід дає змогу уникнути звуженого розуміння цифрового суверенітету як виключно технічного або безпекового питання.

На наш погляд, доцільно виокремити п'ять взаємопов'язаних складових цифрового суверенітету.

Перша - конституційно-інституційна. Вона охоплює здатність держави здійснювати публічну владу в цифровому середовищі відповідно до принципів народовладдя, законності, поділу влади та верховенства права. Цифрові інструменти мають підвищувати ефективність управління, але не повинні підміняти встановлені законом процедури або позбавляти людину можливості оскаржувати рішення органів влади.

Друга - інфраструктурна. Вона передбачає захищеність державних інформаційних систем, електронних реєстрів і критично важливих комунікаційних мереж. Для України це означає необхідність забезпечувати безперервність роботи цифрових сервісів, розробляти механізми відновлення інформаційних систем після кібератак і зменшувати ризики критичної залежності від окремих постачальників технологій.

Третя - інформаційно-правова. Її зміст полягає у встановленні належних правил збирання, зберігання, обробки та передачі даних. При цьому державний контроль над інформаційними ресурсами має здійснюватися з урахуванням конституційних гарантій приватності, свободи слова та доступу до інформації.

Четверта - безпекова. Вона охоплює спроможність держави запобігати кіберзагрозам, виявляти втручання в інформаційні системи та забезпечувати належне реагування на інциденти. Проте безпекові заходи повинні мати чітку правову основу й не використовуватися як універсальне виправдання для обмеження основоположних прав.

П'ята - правозахисна. Вона передбачає доступність цифрових послуг, недискримінаційний характер автоматизованих процедур, прозорість рішень, можливість їх оскарження та наявність ефективного судового захисту.

Важливо підкреслити, що цифровий суверенітет не означає повної технологічної ізоляції. Сучасна цифрова економіка ґрунтується на міжнародній

співпраці, обміні даними та використанні технологій, розроблених різними суб'єктами. Тому сама по собі залежність від іноземного програмного забезпечення або хмарного сервісу не свідчить про втрату державного суверенітету. Проблема виникає тоді, коли така залежність унеможливорює належне виконання державою своїх функцій, створює неприйнятні ризики для безпеки інформації або позбавляє її можливості забезпечити безперервність критичних послуг.

З огляду на це, державна політика має бути спрямована не на безумовну відмову від зовнішніх технологій, а на оцінювання ризиків, забезпечення сумісності систем, належний захист даних і наявність альтернативних механізмів функціонування критичної інфраструктури. Окремої уваги потребує використання штучного інтелекту органами публічної влади. Автоматизовані системи можуть спрощувати адміністративні процедури, однак їх застосування створює ризики алгоритмічної дискримінації, помилкових рішень і непрозорого розподілу прав та обов'язків. Тому рішення, які істотно впливають на права, свободи або законні інтереси людини, повинні супроводжуватися належними гарантіями пояснюваності, людського контролю та оскарження. Використання алгоритмів не звільняє орган державної влади від відповідальності за законність власних рішень.

Проведене дослідження дає підстави стверджувати, що цифровий суверенітет держави є важливою категорією сучасного конституційного права, зміст якої формується під впливом цифровізації публічного управління, розвитку технологій і трансформації механізмів реалізації державної влади.

По-перше, цифровий суверенітет доцільно розглядати як функціональний вимір державного суверенітету, що характеризує спроможність держави здійснювати свої конституційні повноваження в цифровому середовищі,

захищати інформаційні ресурси та забезпечувати стійкість критичної цифрової інфраструктури.

По-друге, чинне законодавство України регулює окремі складові цифрового суверенітету, зокрема кібербезпеку, захист персональних даних і функціонування публічних електронних реєстрів. Водночас комплексне осмислення цифрового суверенітету потребує узгодження цих напрямів із конституційними принципами законності, народовладдя, верховенства права та поваги до людської гідності.

По-третє, практика Європейського суду з прав людини та нормативні акти Європейського Союзу і Ради Європи засвідчують необхідність поєднання цифрової безпеки з належними гарантіями приватності, свободи вираження поглядів і правового захисту. Цифровий суверенітет не може бути підставою для необмеженого державного контролю над інформацією та комунікаціями.

По-четверте, цифрова незалежність не означає відмови від міжнародної технологічної співпраці. Її основним призначенням є забезпечення спроможності держави управляти цифровими ризиками, зменшувати критичні залежності та підтримувати безперервність виконання своїх функцій.

З метою вдосконалення правового регулювання вважаємо доцільним:

1. Розробити законодавче визначення цифрового суверенітету держави, закріпивши його зміст, основні принципи та співвідношення з державним суверенітетом і конституційними правами людини.
2. Запровадити системну оцінку цифрових залежностей критично важливих державних інформаційних систем, передбачивши вимоги до безперервності роботи, захисту даних і відновлення після кібератак.

3. Продовжити наближення законодавства України до європейських стандартів захисту персональних даних, управління даними та регулювання штучного інтелекту з урахуванням міжнародних зобов'язань України.

4. Удосконалити правові гарантії використання автоматизованих систем у публічному управлінні, забезпечивши належну прозорість, людський контроль і можливість оскарження рішень, що впливають на права та законні інтереси людини.

5. Посилити парламентський, судовий та інституційний контроль за заходами цифрового спостереження й обробки інформації, забезпечуючи дотримання принципів законності, необхідності та пропорційності.

Список використаних джерел

1. Pohle J., Thiel T. Digital sovereignty. *Internet Policy Review*. 2020. Vol. 9, no. 4. DOI: <https://doi.org/10.14763/2020.4.1532>. URL: <https://policyreview.info/concepts/digital-sovereignty>.
2. Roberts H., Cows J., Casolari F., Morley J., Taddeo M., Floridi L. Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*. 2021. Vol. 10, no. 3. P. 1–26. DOI: <https://doi.org/10.14763/2021.3.1575>. URL: <https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies>.
3. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
5. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
6. Про публічні електронні реєстри : Закон України від 18 листопада 2021 р. № 1907-IX. URL: <https://zakon.rada.gov.ua/laws/show/1907-20#Text>.
7. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп/2012 у справі щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
9. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). *Official Journal of the European Union*. 2022. L 152. P. 1–44. URL: <https://eur-lex.europa.eu/eli/reg/2022/868/oj>.
10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

11. European Court of Human Rights. *Big Brother Watch and Others v. the United Kingdom* [GC]. Applications nos. 58170/13, 62322/14 and 24960/15. Judgment of 25 May 2021. URL: <https://hudoc.echr.coe.int/eng?i=001-210077>.
12. Council of Europe. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. CETS No. 225. Vilnius, 5 September 2024. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.

Дата першого надходження рукопису до видання: 18.10.2026

Дата прийняття до друку рукопису після рецензування: 20.10.2026

Дата публікації: 27.10.2026

УДК 342.7:364.4-056.26(477)

ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ПРАВ ОСІБ З ІНВАЛІДНІСТЮ В СУЧАСНИХ ДЕРЖАВНО-ПОЛІТИЧНИХ УМОВАХ

Музичук Микола,
аспірант ВЗО «Університет економіки та права «КРОК»

Повномасштабна війна в Україні зумовила виникнення нових викликів у сфері забезпечення та захисту прав людини. Особливої уваги потребують права осіб з інвалідністю, оскільки воєнні дії посилюють наявні соціальні бар'єри та створюють додаткові перешкоди для реалізації їхніх прав. О.Трухан вказує, про те, що «прикро констатувати той факт, що кожного дня кількість людей, які зазнали поранень, збільшується. Для багатьох українців наслідки втрати здоров'я мають незворотний характер, - вони отримують інвалідність» [1].

Руйнування житлової, медичної та транспортної інфраструктури, вимушене переміщення, обмежений доступ до реабілітаційних послуг і цифрових ресурсів можуть призводити до поглиблення соціальної нерівності та дискримінації.

Особливу увагу заслуговує право на працю. Р. Кокош вказує, що «роботодавці часто бояться брати на роботу осіб з інвалідністю, вважаючи, що вони зіштовхнуться з серйозними труднощами при створенні відповідних умов. В цьому контексті важливо об'єднати зусилля роботодавців та неурядових організацій щодо залучення державного фінансування, зокрема, коли розумне пристосування стає надмірним чи невиправданим тягарем для роботодавців»[2].

Правове забезпечення прав осіб з інвалідністю в умовах війни має ґрунтуватися на принципах рівності, недискримінації, поваги до людської гідності та доступності. Важливе значення в цьому контексті має Конвенція

ООН про права осіб з інвалідністю, яка передбачає обов'язок держави вживати необхідних заходів для захисту таких осіб у ситуаціях ризику, зокрема під час збройних конфліктів і гуманітарних надзвичайних ситуацій.

Однією з ключових проблем залишається недостатня доступність укриттів, евакуаційних маршрутів, пунктів тимчасового розміщення та інформації про небезпеку. Для людей із порушеннями мобільності, слуху, зору або інтелектуальними порушеннями недостатність систем оповіщення та евакуаційної інфраструктури може становити безпосередню загрозу життю. Тому необхідно забезпечувати універсальний дизайн укриттів, дублювання повідомлень про небезпеку в різних форматах і розроблення планів евакуації з урахуванням індивідуальних потреб людей з інвалідністю.

Іншим важливим напрямом є забезпечення безперервності медичної допомоги та реабілітації. В умовах бойових дій особи з інвалідністю можуть втрачати доступ до лікарських засобів, допоміжних засобів реабілітації, протезування, психологічної підтримки та спеціалізованих медичних послуг. У зв'язку з цим доцільно вдосконалювати механізми оперативного визначення індивідуальних потреб, забезпечення необхідними засобами реабілітації та організації допомоги під час переміщення між громадами. Водночас особливу увагу слід приділяти ветеранам і цивільним особам, які набули інвалідності внаслідок війни, не допускаючи нерівного доступу до послуг через місце проживання або соціальний статус.

Окремого розгляду потребує доступність державних і соціальних послуг. Цифровізація адміністративних процедур може спростити взаємодію громадян із державою, однак за відсутності доступних вебсайтів, сумісності з допоміжними технологіями та альтернативних способів отримання послуг вона здатна створювати додаткові бар'єри. Тому цифрові сервіси мають відповідати

вимогам доступності, а особам, які не можуть скористатися ними самотійно, необхідно забезпечувати доступні альтернативні канали обслуговування.

Не менш важливим є захист прав внутрішньо переміщених осіб з інвалідністю. Вимушена зміна місця проживання часто супроводжується втратою звичних соціальних зв'язків, труднощами з пошуком доступного житла та обмеженням можливостей працевлаштування. Удосконалення правових механізмів у цій сфері має передбачати оцінювання доступності місць тимчасового проживання, узгодження соціальних і реабілітаційних послуг між громадами та врахування індивідуальних потреб під час надання допомоги.

Важливою умовою ефективного захисту прав осіб з інвалідністю є їх безпосереднє залучення до формування та реалізації державної політики. Органи державної влади й місцевого самоврядування повинні створювати реальні можливості для участі громадських об'єднань осіб з інвалідністю в обговоренні рішень щодо відбудови, цивільного захисту, соціального забезпечення та доступності інфраструктури. Такий підхід дасть змогу враховувати практичний досвід людей, яких безпосередньо стосуються відповідні рішення.

Отже, війна посилює системні проблеми реалізації прав осіб з інвалідністю та потребує комплексного вдосконалення правового регулювання. Пріоритетними напрямками мають стати забезпечення доступності укриттів і евакуації, безперервності медичної допомоги та реабілітації, інклюзивності цифрових і соціальних послуг, а також належного захисту внутрішньо переміщених осіб з інвалідністю. Важливо не лише закріплювати відповідні гарантії в законодавстві, а й забезпечувати дієві механізми їх виконання, фінансування, моніторингу та громадського контролю. Реалізація цих заходів

сприятиме зміцненню прав людини, зменшенню дискримінації та формуванню інклюзивного середовища навіть за умов воєнного стану.

Список використаних джерел

1. Лідіч Б. В. Деякі питання соціального захисту осіб з інвалідністю в умовах воєнного стану. *Сучасний науковий журнал*. 2024. № 5 (3). С. 8-14. DOI: <https://doi.org/10.36994/2786-9008-2024-5-1>
2. Кокош Р. Г. Гарантії забезпечення права на працевлаштування осіб з інвалідністю в умовах воєнного стану. *Прикарпатський юридичний вісник*. 2025. № 1. С. 54-59. DOI: <https://doi.org/10.32782/pyuv.v1.2025.11>

Дата першого надходження рукопису до видання: 18.10.2026

Дата прийняття до друку рукопису після рецензування: 20.10.2026

Дата публікації: 27.10.2026

© Музичук М., 2026

УДК 342.8:004.738.5(477)

ЕЛЕКТРОННЕ ГОЛОСУВАННЯ НА ВИБОРАХ: КОНСТИТУЦІЙНІ ГАРАНТІЇ, РИЗИКИ ТА МЕЖІ ЦИФРОВІЗАЦІЇ ВИБОРЧОГО ПРОЦЕСУ

Рішко Євгенія Павлівна

здобувачка другого (магістерського) рівня вищої освіти

спеціальності D8 «Право»,

Ужгородський університет,

<https://orcid.org/0009-0000-4368-0227>

Цифрова трансформація публічного управління протягом останніх десяти років надає все більшої актуальності питанню використання інформаційно-комунікаційних технологій у виборчому процесі. Електронне голосування потенційно здатне спростити участь громадян у виборах, підвищити доступність виборчих процедур для осіб, які перебувають за кордоном або мають обмежену мобільність, а також оптимізувати підрахунок голосів. Водночас перенесення волевиявлення в цифрове середовище створює ризики, які безпосередньо стосуються конституційної легітимності виборів. Такими ризиками постає втручання в інформаційні системи, порушення таємниці голосування, цифрова нерівність та неможливість незалежно перевірити результати. Для України ця проблематика має особливе значення у зв'язку з необхідністю забезпечення стійкості демократичних інститутів в умовах воєнних загроз, небезпеки в кіберпросторі та значного переміщення громадян. Однак технологічна доцільність не може підміняти конституційні вимоги до виборів.

Відповідно до статті 71 Конституції України вибори до органів державної влади та органів місцевого самоврядування є вільними і відбуваються на основі

загального, рівного і прямого виборчого права шляхом таємного голосування, а виборцям гарантується вільне волевиявлення. Стаття 38 Конституції України вказує, що громадяни мають право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування [1]. В контексті цих провідних стосовно можливості обирати та бути обраним статей Конституції вбачається, що для реалізації ідеї електронного голосування необхідно дотримати конституційні вимоги та належним чином забезпечити вільність таких виборів, загальне, рівне і пряме виборче право, таємність голосування, вільність волевиявлення виборців. Саме ці вимоги мають спрямовувати рух думок та ідей, проєктування системи електронного голосування та її втілення. Ці конституційні засади є фундаментом права обирати та бути обраним, тому коли постає питання видозміни цього права та його модифікації в зв'язку з вимогами й тенденціями сучасності, повинне поставати також і питання забезпечення непорушного й безумовного дотримання й гарантування відповідних конституційних засад.

Отже, основна наукова проблема полягає у визначенні конституційно допустимих меж цифровізації голосування. Вона потребує відповіді на принципове питання: чи може держава гарантувати реальне здійснення виборчих прав у цифровому середовищі з тією самою мірою юридичної визначеності, таємності, рівності й суспільної довіри, яка вимагається від традиційного голосування?

У науковій літературі електронне голосування розглядається як неоднорідна категорія. Воно охоплює використання електронних пристроїв на виборчій дільниці, автоматизоване зчитування паперових бюлетенів та дистанційне голосування через Інтернет. Остання модель створює найбільш

комплексні правові проблеми, оскільки голосування відбувається поза контрольованим виборчим приміщенням, а держава не може безпосередньо спостерігати за умовами волевиявлення.

Дослідження П. Егіна, М. Солвака, Я. Віллемсона та П. Вінкеля щодо досвіду Естонії засвідчує, що результативність інтернет-голосування залежить не лише від технології, а й від розвиненої цифрової інфраструктури, організаційної спроможності держави та довіри до виборчих інституцій [2].

Інтернет-голосування використовується в Естонії на загальнонаціональних, європейських і місцевих виборах із 2005 року. Електронне голосування (i-voting) є обов'язковою альтернативою традиційному голосуванню на паперових бюлетенях і доступне протягом визначеного періоду дострокового голосування – з десятого до четвертого дня перед днем виборів. Виборці можуть проголосувати з будь-якого комп'ютера, підключеного до Інтернету, незалежно від свого місцезнаходження у світі. На вебсторінці виборів виборець спочатку завантажує програму для голосування та запускає її на власному комп'ютері. Далі він проходить автентифікацію за допомогою естонської ID-картки або мобільного цифрового посвідчення особи (mobile-ID), переглядає список кандидатів, які балотуються у відповідному виборчому окрузі, робить свій вибір, шифрує його та підтверджує голос цифровим підписом. Увесь процес у середньому триває менше двох хвилин [3]. Важливою особливістю цієї системи є те, що протягом періоду дострокового голосування виборці можуть необмежену кількість разів змінювати свій електронний голос. Кожне нове голосування анулює всі попередні електронні голоси цього виборця. Голосування на виборчій дільниці протягом періоду дострокового голосування робить недійсним бюлетень, поданий через Інтернет. Такі правила було запроваджено для забезпечення таємниці голосування:

виборець, якого примусили або залякали з метою схилити до голосування певним чином, може подати новий голос, змінивши свій попередній вибір. До 2021 року особи, які проголосували через Інтернет, не могли голосувати в день виборів, оскільки їхні прізвища вилучалися з відповідних списків виборців. Починаючи з 2021 року, такі виборці отримали можливість проголосувати в день виборів за допомогою паперового бюлетеня, що призводить до анулювання їхнього електронного голосу [2, с.3].

Естонія має комплексну нормативно-правову базу, яка забезпечує можливість електронного голосування через Інтернет. Закон про документи, що посвідчують особу (Identity Documents Act), ухвалений у 1999 році, згодом було доповнено детальними положеннями щодо цифрових посвідчень особи, зокрема цифрової ідентифікації за допомогою mobile-ID. Закон про цифрові підписи (Digital Signatures Act), ухвалений у 2000 році, регулює використання цифрових підписів, які мають юридичну силу, а також надання послуг із сертифікації та електронного засвідчення часу. Закон про Реєстр населення (Population Register Act) і Закон про захист персональних даних (Personal Data Protection Act) регулюють використання даних, внесених до Реєстру населення – основної державної бази даних, що містить інформацію про всіх громадян і мешканців Естонії [2, с.4].

Впродовж двох десятиліть законодавство та технічне регулювання електронного голосування розвивалися шляхом внесення низки змін, які відображали як національні підходи до вдосконалення системи, так і рекомендації Бюро з демократичних інститутів і прав людини (БДПІЛ) Організації з безпеки і співробітництва в Європі (ОБСЄ). На запрошення уряду Естонії місії ОБСЄ/БДПІЛ з оцінювання виборів або спеціалізовані групи експертів спостерігали за всіма чотирма виборами до Рійгікогу, під час яких

застосовувалося інтернет-голосування (у 2007, 2011, 2015 і 2019 роках), та готували відповідні звіти [4, 5]. У звіті ОБСЄ/БДПЛ за результатами виборів 2015 року зазначалося, що електронне голосування організовувалося ефективно та відповідно до законодавчої бази, водночас було наголошено на необхідності вжиття додаткових заходів для підвищення прозорості та підзвітності [4, с.1]. У 2015 році Рійгікогу розпочав новий цикл обговорень, спрямованих на підвищення можливості перевірки результатів голосування та прозорості виборчого процесу шляхом комплексного перегляду системи організації виборів. Систему управління виборами було докорінно реформовано: наглядові повноваження Національного виборчого комітету (National Electoral Committee, NEC) відокремили від функцій безпосередньої організації виборів, які передали новоствореній установі – Державній виборчій службі (State Electoral Office, SEO), що діє при Канцелярії парламенту. Крім того, електронне голосування було тісніше інтегровано до державної екосистеми електронного врядування шляхом розмежування технічних функцій оператора зі збору голосів і функцій організації виборів, покладених на SEO. Також було розроблено оновлену технологічну інфраструктуру електронного голосування, яку вперше використали на місцевих виборах 2017 року. ОБСЄ/БДПЛ позитивно оцінило ці зміни. У звіті за результатами виборів до Рійгікогу 2019 року організація дійшла висновку, що конструкція системи інтернет-голосування, яка існує наразі, є суттєвим удосконаленням порівняно з попередніми версіями, зокрема з погляду забезпечення цілісності системи та таємниці голосування [5, с.1].

Естонські суди здійснювали перевірку конституційності електронного голосування та підтвердили його відповідність Конституції, дійшовши висновку, що законодавчі положення про інтернет-голосування відповідають конституційним вимогам щодо проведення вільних, загальних, рівних і прямих

виборів із таємним голосуванням [2, с.5]. Розглянувши подання Президента Республіки, Верховний суд Естонії у 2005 році постановив, що можливість змінити свій електронний голос протягом періоду дострокового голосування не порушує принципу рівності виборів. Крім того, Суд зазначив, що можливість зміни електронного голосу є додатковою гарантією свободи волевиявлення та таємниці голосування, оскільки така можливість зміни робить спроби вплинути на волю виборця незаконними засобами марними й безглуздими та забезпечує важливий засіб відновлення таємниці голосування для будь-якої особи, яка вважає, що конфіденційність її голосу було з будь-якої причини порушено [6].

У такий спосіб досвід Естонії демонструє, що впровадження інтернет-голосування є не стільки питанням технологічного забезпечення виборчого процесу, скільки комплексним завданням, що потребує узгодженого розвитку цифрової інфраструктури, законодавчого регулювання та інституційних гарантій. Принципове значення має не лише доступність електронного волевиявлення, а й наявність механізмів захисту таємниці голосування, перевірки результатів, незалежного нагляду та судового контролю за дотриманням конституційних принципів виборчого права. Водночас естонський досвід засвідчує, що навіть тривале функціонування системи не усуває потреби в її постійному вдосконаленні, посиленні прозорості та нормативному закріпленні процедурних і технічних вимог.

Важливим міжнародним орієнтиром для реалізації системи електронного голосування в державі є Тлумачна декларація Кодексу належної практики у виборчих питаннях щодо цифрових технологій та штучного інтелекту, схваленого Радою з демократичних виборів на її 81-му засіданні (Венеція, 5 грудня 2024 року) та прийнятого Венеціанською комісією на її 141-му пленарному засіданні (Венеція, 6-7 грудня 2024 року), яка акцентує на тому, що

досягнення у сфері цифрових технологій та штучного інтелекту відкрили нові можливості для демократії, водночас породивши нові виклики, які було важко навіть уявити на момент ухвалення у 2002 році Кодексу належної практики у виборчих справах [7, пункт 28]. Тлумачна конвенція посиляється на Спільну доповідь Венеційської комісії та Директорату інформаційного суспільства і протидії злочинності Генерального директорату з прав людини та верховенства права (DGI) за 2019 рік щодо цифрових технологій і виборів, де зазначено, що цифрові (або «нові») технології та соціальні мережі докорінно змінили спосіб взаємодії людей і реалізації ними свободи вираження поглядів та свободи інформації, а також інших пов'язаних із ними основоположних прав, які іноді можуть суперечити одне одному. Особи, які користуються соціальними мережами, можуть використовувати Інтернет для організації діяльності та висунення вимог щодо якісніших послуг, більшої прозорості й реальної участі в політичному житті. Люди в усьому світі тепер здатні формувати глобальні уявлення, включати певні питання до національного політичного порядку денного та сприяти політичній активності. Ця цифрова трансформація змінює характер відносин між державами та громадянами [8, пункт 4]. З одного боку, нові віртуальні інструменти можуть використовуватися, а іноді й справді використовуються проти виборів із метою придушення виборчої активності, фальсифікації результатів голосування та викрадення інформації про виборців; проти політичних партій і політиків – для здійснення кіберрозвідки з метою примусу й маніпулювання, а також публічної дискредитації окремих осіб; проти традиційних засобів масової інформації та соціальних мереж – для поширення дезінформації й пропаганди та формування поглядів виборців [8, пункт 143]. З іншого боку, цифрові інструменти й технології відкривають широкий спектр

можливостей і можуть підвищувати ефективність та результативність у багатьох сферах, зокрема у виборчих процесах [7, пункт 31].

Як зазначено в нещодавно ухваленій Рамковій конвенції Ради Європи про штучний інтелект і права людини, демократію та верховенство права (CETS № 225), розвиток науки й технологій та глибокі зміни, зумовлені діяльністю на різних етапах життєвого циклу систем штучного інтелекту мають потенціал сприяти людському процвітання, добробуту окремих осіб і суспільства, сталому розвитку, гендерній рівності та розширенню можливостей усіх жінок і дівчат, а також досягненню інших важливих цілей та реалізації інтересів шляхом стимулювання прогресу й інновацій [9, преамбула].

Принципи, закріплені в Кодексі належної практики у виборчих справах набувають особливого значення в цифровому середовищі, оскільки використання цифрових технологій може створювати безпрецедентні можливості для їх повноцінної реалізації. Водночас цифрові технології здатні істотно посилювати ризики для цих самих принципів і умов їх дотримання, зокрема щодо процесуальних гарантій [7, пункт 32]. Загалом держави зобов'язані запроваджувати та підтримувати заходи, спрямовані на забезпечення того, щоб цифрові технології, включно зі штучним інтелектом, не використовувалися для підриву цілісності, незалежності та ефективності демократичних інституцій і виборчих процесів. Одним зі способів реалізації цього завдання є покладення на орган управління виборами обов'язку забезпечувати цілісність виборчої системи, а отже, і надійність виборчих процесів та їх результатів [7, пункт 33].

Право на вільні вибори закріплене також у статті 3 Протоколу до Конвенції про захист прав людини і основоположних свобод, де зазначається, що Високі Договірні Сторони зобов'язуються проводити вільні вибори з

розумною періодичністю шляхом таємного голосування в умовах, які забезпечують вільне вираження думки народу у виборі законодавчого органу [10]. Це свідчить про те, що в будь-якому випадку, навіть якщо сучасне нормативне регулювання формує підхід про те, що спосіб організації виборів може змінюватися, зміст конституційних гарантій попри все залишається незмінним.

З огляду на розглянуті міжнародні документи та реальну практику застосування системи електронного голосування в європейському просторі, можна виокремити два основні критерії конституційності електронного голосування. Першим таким критерієм є збереження вільного волевиявлення. Свобода голосування означає не лише відсутність прямого примусу, а й наявність реальної можливості самостійно сформулювати та реалізувати вибір. Під час дистанційного голосування особа може перебувати під контролем роботодавця, члена сім'ї або іншої заінтересованої особи. За таких обставин технічне підтвердження особи виборця не гарантує свободи його волевиявлення, тому у випадку запровадження системи електронного голосування необхідно насамперед подбати про забезпечення такого вільного волевиявлення кожній особі. Другим критерієм є таємниця голосування. Необхідно розмежовувати автентифікацію виборця та ідентифікацію його вибору: система має перевіряти право особи проголосувати, не створюючи можливості пов'язати її особу з конкретним голосом. Збереження такого розмежування повинно забезпечуватися не лише декларативними нормами, а й архітектурою системи, правилами доступу до даних, незалежним аудитом та відповідальністю за неправомірне втручання.

Показовою в характеристиці виборів згідно з конституційними засадами є практика Конституційного Суду України. Відповідно до рішення Великої палати

Конституційного Суду України № 3-р/2017 від 21 грудня 2017 року «держава зобов’язана забезпечити вільне волевиявлення громадян України та повагу до результатів такого волевиявлення шляхом належної регламентації й організації виборчого процесу на демократичних засадах та з дотриманням демократичних процедур, а також шляхом впровадження ефективного контролю за здійсненням таких процедур, що має унеможливити будь-які зловживання та маніпуляції, у тому числі з виборчими списками від партій» [11]. По суті Конституційний Суд України не вказує, в який спосіб чи в якому форматі має бути забезпечено вільне волевиявлення та повага до його результатів. Він лише наголошує, що для такого забезпечення виборчий процес має бути належним чином регламентований і організований на демократичних засадах та з ефективним контролем, що безумовно може бути реалізовано й шляхом проведення електронного голосування на виборах. Суд установлює чіткі вказівки того, що має бути дотримано та забезпечено під час голосування на виборах, але залишає диспозитивною можливість реалізувати таке голосування в будь-який не заборонений законом спосіб, головне – дотримати всі конституційні засади та принципи.

Європейський Суд з прав людини не надто багатослівний щодо процедури електронного голосування на виборах, але дещо в контексті електронного голосування все ж сказав, і тут знову необхідно повернутись до Естонії. У справі «AUSAD VALIMISED MTÜ v. Estonia» зазначається, що естонська громадська організація Ausad Valimised MTÜ у 2013 році провела кампанію проти електронного голосування. На плакатах були розміщені твердження про те, що електронний голос можуть змінити або видалити, а також гасло про загрозу, яку електронне голосування може становити для незалежності Естонії. Орган із захисту прав споживачів оштрафував організацію на 1600 євро за

порушення законодавства про рекламу. Національний суд залишив рішення в силі по суті, але зменшив штраф до 800 євро. Організація звернулася до ЄСПЛ, стверджуючи, що притягнення її до відповідальності порушило право на свободу вираження поглядів, гарантоване статтею 10 Європейської конвенції з прав людини. Натомість Суд визнав заяву неприйнятною. Причиною стало не оцінювання законності електронного голосування чи обмеження критики цієї системи, а розголошення заявником конфіденційної інформації про переговори щодо дружнього врегулювання спору. Суд кваліфікував це як зловживання правом на подання індивідуальної заяви відповідно до статті 35 Конвенції [12]. Отже, ЄСПЛ не сформулював у цій справі правової позиції щодо відповідності електронного голосування вимогам Конвенції, він не висловив позицію за чи проти електронного голосування, тому можна зробити висновок, що запровадження електронного голосування вимагає врахування не лише технологічних і виборчо-правових питань, а й гарантій свободи вираження поглядів у публічній дискусії про безпеку та достовірність електронного волевиявлення. В іншому рішенні в справі «CASE OF MUGEMANGANGO v. BELGIUM» Велика палата ЄСПЛ нагадує, що поняття «вільні вибори» опиняється під загрозою лише за наявності доказів процесуальних порушень, які можуть спотворити вільне волевиявлення народу, та за умови, що скарги на такі порушення не були ефективно розглянуті на національному рівні [13]. Тобто ЄСПЛ не вказує, що певний спосіб, форма голосування на виборах призводять до появи загрози вільним виборам, адже це залежить не від способу (голосування з використанням паперових бюлетенів чи електронне голосування), а від наявності процесуальних порушень, що впливають на вільне волевиявлення, а це може мати місце під час будь-якого способу голосування на виборах.

Українські науковці, розглядаючи можливість створення в нашій державі системи електронного голосування на виборах, зазначають, що «поряд із збільшенням зручності виборчої процедури і для виборців, і для членів виборчих комісій, відбувається зменшення ризиків втручання в процедуру підрахунку голосів, який тепер відбувається автоматизовано. Таким чином, зменшується вплив особистісного фактору, тобто виконання процедури підрахунку голосів делегується машинній системі, і потенційно неетичні й недоброчесні дії членів виборчої комісії не можуть бути зреалізовані. Проте, видається, що збільшуються ризики, пов'язані з ідентифікацією виборців, яка здійснюється лише за документами (сканування біометричних параметрів не є обов'язковим), візуальну перевірку відповідності документів особі, що їх надає, пристрій для голосування не здійснює. Це створює ризики використання «крадіжки особистостей», в тому числі й для незаконного голосування. Такого роду дії породжують значну кількість етичних проблем, пов'язаних із неможливістю зробити волевиявлення особою, особистість якої вкрадено, а також складністю у визначенні відповідальності за результат вибору, який був здійснений від імені особи, але не самою особою. Необхідно зважати і на той факт, що вплив на підрахунок результатів виборів може відбуватися й на більш пізніх етапах, якщо комп'ютерні системи зберігання результатів голосування чи навіть автономні машини для голосування виявляться уразливими для зовнішнього втручання» [14, с.142].

Електронне голосування розглядається дослідниками як пов'язане з численними ризиками в сфері кіберзахисту. Зокрема, існує небезпека хакерських атак, які можуть спричинити спотворення результатів або викрадення конфіденційної інформації виборців. Значну загрозу можуть становити спроби втручання з боку іноземних держав або організованих груп,

що мають на меті вплинути на підсумки голосування для реалізації власних політичних чи стратегічних інтересів [15, с.153]. До того ж інформаційна інфраструктура в різних регіонах країни є неоднорідною, що впливає на доступ до електронного голосування, а відсутність стабільного інтернету або сучасного обладнання в сільській місцевості ускладнює можливість забезпечити рівну участь у виборах. До цього додається і старіння техніки, що обмежує ефективність реалізації електронного голосування на практиці [16, с.46]. Ще одним ризиком постає той факт, що «для осіб похилого віку електронне голосування може стати серйозним бар'єром. Обмежений доступ до цифрових технологій, слабка комп'ютерна грамотність або повна її відсутність часто позбавляють старших громадян можливості самостійно взяти участь у виборах. Це ставить під загрозу принцип інклюзивності виборчого процесу» [17, с.23].

Підсумовуюче все розглянуте та проаналізоване вище, можна узагальнити, що конституційність електронного голосування має визначатися за принципом функціональної еквівалентності гарантій: цифрова процедура повинна забезпечувати не формальне відтворення традиційних правил, а належний рівень захисту виборчих прав. Якщо технологічна модель не дозволяє надійно підтвердити достовірність результатів, створює неприйнятний ризик розкриття таємниці голосу, порушує вільність виборів чи інші конституційні засади, її зручність не може виправдати застосування. При цьому не слід ототожнювати електронне голосування з усією цифровізацією виборчого процесу. Електронні реєстри виборців, цифрове інформування, автоматизоване передавання протоколів і допоміжні засоби підрахунку можуть упроваджуватися поетапно, якщо для кожного з них визначено правову основу, межі використання та засоби контролю. Натомість дистанційне голосування через Інтернет потребує окремого, значно суворішого обґрунтування, оскільки

поєднує технічні ризики з неможливістю безпосередньо контролювати умови волевиявлення.

Для України доцільно передбачити наступні напрями нормативного вдосконалення. По-перше, законодавче регулювання має встановлювати чітке визначення різних видів електронного голосування, вимоги до сертифікації систем, незалежного аудиту, кібербезпеки, зберігання даних та відповідальності за втручання. Необхідно закріпити обов'язок публікувати зрозумілі для громадськості звіти про результати незалежної перевірки системи. По-друге, запровадження дистанційного голосування має супроводжуватися гарантіями добровільності та доступності: збереженням альтернативного способу голосування, недопущенням дискримінації осіб із низькою цифровою грамотністю, а також процедурою реагування на технічні збої, яка не дає можливості довільно змінювати результати. По-третє, необхідно забезпечити незалежну перевірку результатів. У межах технічно здійсненої моделі вона повинна дозволяти підтверджувати, що голоси враховані належним чином, не розкриваючи вибору конкретного виборця. У разі суттєвого інциденту закон має передбачати порядок збереження доказів, незалежного розслідування, судового контролю та визначення правових наслідків порушення. По-четверте, доцільно передбачити поетапне тестування нових технологій без автоматичного надання результатам експерименту юридичної сили на загальнодержавних виборах. Пілотні проєкти мають супроводжуватися оцінкою ризиків, незалежним спостереженням, публічним звітуванням і чіткими критеріями припинення експлуатації системи в разі виявлення критичних вразливостей. Нарешті, законодавець повинен виходити з того, що довіра до виборів формується не самим фактом застосування сучасної технології, а можливістю незалежно перевірити її роботу, встановити відповідальних за порушення та забезпечити

ефективне поновлення виборчих прав. Цифровізація має бути інструментом реалізації народовладдя, а не підставою для послаблення конституційних гарантій.

Таким чином, електронне голосування є потенційним засобом модернізації виборчого процесу, проте його впровадження потребує оцінювання не лише технічної ефективності, а й конституційної сумісності. Загальне, рівне, пряме виборче право, таємність голосування та свобода волевиявлення залишаються обов'язковими незалежно від способу голосування та підрахунку голосів. Міжнародні нормативно-правові акти, практика Європейського Суду з прав людини і Конституційного Суду України, та сучасний науковий погляд дають підстави стверджувати, що легітимність виборів залежить від реальності забезпечення демократичних гарантій та таких вимог як прозорість, надійність та безпека. Основною умовою допустимості електронного голосування має бути функціональна еквівалентність конституційних гарантій. Для України найбільш обґрунтованим напрямом є поступова цифровізація допоміжних етапів виборчого процесу з одночасним розвитком правового й технічного контролю. Дистанційне голосування через Інтернет має розглядатися окремо, із застосуванням посилених вимог до захисту таємниці голосування, протидії примусу, кібербезпеки та незалежного аудиту. За відсутності можливості забезпечити ці гарантії технологічна зручність не може вважатися достатньою підставою для впровадження відповідної моделі.

Список використаних джерел

1. Конституція України: від 28.06.1996р. (ред. від 01.01.2020р.). Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Ehin P., Solvak M., Willemson J., Vinkel P. Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*. 2022. Vol. 39, Issue 4. Article 101718. 14 p. DOI: <https://doi.org/10.1016/j.giq.2022.101718>
3. Heiberg, S., Parsovs, A., & Willemson, J. (2015). Log Analysis of Estonian Internet Voting 2013-2014. In R. Haenni, R. E. Koenig, & D. Wikström (Eds.), *E-Voting and Identity – 5th international conference, voteid 2015*, Bern, Switzerland proceedings (pp. 19–34). Cham: Springer. URL: https://link.springer.com/chapter/10.1007/978-3-319-22270-7_2
4. OSCE/ODIHR. (2015). OSCE/ODIHR election expert team report on parliamentary elections 1.03.2015. URL: <https://www.osce.org/files/f/documents/a/4/160131.pdf>
5. OSCE/ODIHR. (2019). OSCE/ODIHR election expert team report on parliamentary elections 3.03.2019. URL: <https://www.osce.org/files/f/documents/8/e/424229.pdf>
6. Supreme Court of Estonia. (2005). Supreme court judgement 3-4-1-13-05 1.09.2005 on constitutionality of the Estonian internet voting system. URL: <https://rikos.rik.ee/Lahendid?.asjaNr=3-4-1-4-11>
7. Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence, approved by the Council for Democratic Elections at its 81st meeting (Venice, 5 December 2024) and adopted by the Venice Commission at its 141st Plenary Session (Venice, 6-7 December 2024). Strasbourg, 10 December 2024. Opinion No. 1171/2024. 16 p. URL: <https://www.coe.int/en/web/venice-commission/-/cdl-ad-2024-044-e>
8. Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and

15. Панкратова В.О. Електронне голосування як елемент електронної демократії: досвід країн ЄС. Аналітично-порівняльне правознавство. 2023. № 6. С. 152–155. URI: <https://essuir.sumdu.edu.ua/handle/123456789/93900>
16. Войнова Е. О. Упровадження електронного голосування: позитивні та негативні риси електронних виборів Політикус: наук. журнал. 2020. №5. С. 44–49. URL: https://www.politicus.od.ua/5_2020/8.pdf
17. Дятлик О.О. Вплив електронного голосування на результати виборів (на прикладі країн Європи). Київський столичний університет імені Бориса Грінченка. Київ, 2025. 76 с. URI: <https://elibrary.kubg.edu.ua/id/eprint/52465>

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.7:004.738.5(477)

ПРАВО НА ДОСТУП ДО ІНТЕРНЕТУ ЯК НОВІТНЄ КОНСТИТУЦІЙНЕ ПРАВО ЛЮДИНИ: ДОКТРИНАЛЬНІ ТА НОРМАТИВНІ ПІДХОДИ

Самойленко Юлія В'ячеславівна,
студентка юридичного факультету,
2 групи 2 курс магістратури,
Ужгородський університет

Стрімкий розвиток цифрових технологій змінив значення Інтернету: з інструменту для розваг і спілкування він став невід'ємною частиною повсякденного життя людини. Відповідно до Закону України «Про електронні комунікації», мережа Інтернет – це глобальна електронна комунікаційна мережа, призначена для передавання даних та утворена взаємоз'єднаними електронними комунікаційними мережами [1].

Інтернет відкриває доступ до значних обсягів інформації, дає змогу отримувати освіту, спілкуватися, працювати, користуватися державними послугами та брати участь у суспільному житті. Актуальність цієї проблематики полягає в тому, що доступ до Інтернету став важливою умовою реалізації багатьох прав людини. Тому виникає питання, чи можна вважати право на доступ до Інтернету окремим конституційним правом, чи є воно засобом реалізації вже закріплених у Конституції України прав, зокрема права на свободу слова, доступ до інформації та освіти.

У науковій літературі існують різні погляди на правову природу цього права. Зокрема, О. Б. Братасюк та Н. Ф. Ментух у своїй праці «Поняття та класифікація цифрових прав в Україні» розглядають право на доступ до Інтернету як одне з цифрових прав людини. Автори звертають увагу на те, що

розвиток інформаційних технологій зумовлює появу нових суспільних відносин, які потребують належного правового регулювання. При цьому цифрові права можуть розглядатися як окрема група прав людини або як сучасна форма реалізації вже закріплених прав у цифровому середовищі [2, с.58-59]. На нашу думку, обидва підходи мають підстави для існування. З одного боку, доступ до Інтернету безпосередньо пов'язаний із реалізацією права на інформацію, свободи вираження поглядів, тощо. З іншого боку, значення Інтернету в сучасному суспільстві настільки зросло, що виникає потреба в окремих правових гарантіях його доступності. Тому важливо не лише визначити місце цього права в системі прав людини, а й установити, які обов'язки має держава щодо забезпечення доступу до мережі та за яких умов таке право може бути обмежене.

Подібну проблематику досліджував М. І. Марчук у праці «Право на інтернет як базове право людини». Розглядаючи питання правової природи цього права, автор звертається до ідей Джона Стюарта Мілля (британський філософ), відповідно до яких визнання певного блага правом людини передбачає можливість вимагати від суспільства його захисту. Автор також звертає увагу на те, що різні держави по-різному ставляться до забезпечення свободи в Інтернеті. У деяких випадках держава здійснює масштабний контроль над доступом до інформації, обмежуючи поширення певного контенту та використання інтернет-ресурсів. Мова йде про Китайську Народну Республіку, де функціонує система фільтрації та блокування інтернет-контенту, відома як «Великий китайський файрвол». Така практика демонструє, що наявність технічного доступу до мережі ще не гарантує людині можливості вільно отримувати й поширювати інформацію [3, с.117]. На нашу думку, подібні обмеження потребують особливої уваги з погляду захисту свободи вираження

поглядів, оскільки втручання держави в інформаційний простір не повинно перетворюватися на засіб необґрунтованої цензури.

Проаналізувавши законодавство нашої держави можна дійти висновку, що Конституція України прямо не закріплює право на доступ до Інтернету як самостійне конституційне право. Проте стаття 34 Конституції гарантує кожному право на свободу думки і слова, а також право вільно збирати, зберігати, використовувати й поширювати інформацію, а стаття 53 закріплює право на освіту [4]. У сучасних умовах Інтернет є одним із засобів реалізації цих прав, тому його доступність має важливе значення для забезпечення конституційних гарантій. На нашу думку, відсутність в Основному Законі окремої норми про право на доступ до Інтернету не означає, що це питання перебуває поза межами конституційно-правового регулювання. Уже закріплені в Конституції права повинні реалізовуватися незалежно від того, чи відбувається це в традиційному середовищі, чи за допомогою цифрових технологій. Водночас чинні положення не дають вичерпної відповіді на питання щодо обов'язку держави забезпечувати доступність Інтернету для всіх осіб, зокрема тих, які проживають у віддалених населених пунктах або мають обмежені фінансові можливості.

Важливе значення для розуміння права на доступ до Інтернету мають також міжнародні стандарти у сфері захисту прав людини. Зокрема, Рада Європи у Рекомендації CM/Rec(2014)6 щодо посібника з прав людини для користувачів Інтернету наголошує на необхідності забезпечення прав і свобод людини в цифровому середовищі. У пункті 3 закріплено, що Інтернет має цінність як суспільна служба. Тож, документ звертає увагу на те, що права людини, гарантовані Європейською конвенцією з прав людини, мають захищатися і під час користування Інтернетом. Хоча ця Рекомендація не є

міжнародним договором, вона має важливе значення для розуміння європейських підходів до захисту прав користувачів мережі [5].

Звернемося також до практики Європейського суду з прав людини. Зокрема, у справі «Ahmet Yıldırım проти Туреччини» Суд розглядав питання блокування доступу до вебсайтів, унаслідок якого було обмежено доступ і до ресурсу, яким користувався заявник. Суд звернув увагу на те, що такі заходи можуть впливати на право отримувати та поширювати інформацію, гарантоване статтею 10 Європейської конвенції з прав людини [6]. Ця справа показує, що обмеження доступу до інтернет-ресурсів повинні мати належне правове обґрунтування та відповідати вимогам захисту прав людини.

Подібна проблема розглядалася у справі «Cengiz та інші проти Туреччини», яка стосувалася блокування платформи YouTube. Європейський суд з прав людини зазначив, що блокування платформи вплинуло на можливість заявників отримувати та поширювати інформацію, а отже, стосувалося реалізації свободи вираження поглядів [7].

На нашу думку, практика ЄСПЛ є важливою для України, оскільки демонструє необхідність дотримання балансу між законними інтересами держави та правом людини вільно отримувати та поширювати інформацію.

На національному рівні питання доступу до Інтернету безперечно пов'язане із захистом персональних даних. Відповідно до Закону України «Про захист персональних даних», правове регулювання у цій сфері спрямоване на захист основоположних прав і свобод людини під час обробки її персональних даних [8]. Це має особливе значення в умовах активного використання соціальних мереж, електронних сервісів та інших інтернет-ресурсів. Отже, забезпечення прав людини в цифровому середовищі передбачає не тільки

можливість доступу до мережі, а й належний захист приватного життя та персональної інформації.

Важливе значення для розуміння конституційних гарантій у цифровому середовищі має Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012. У ньому Суд розглянув питання співвідношення права на недоторканність особистого і сімейного життя та права на вільне збирання, зберігання, використання і поширення інформації. Зокрема, КСУ звернув увагу на те, що однією з гарантій реалізації інформаційних прав є доступ до інформації, який може забезпечуватися шляхом її оприлюднення на офіційних вебсайтах в Інтернеті [9]. Хоча це рішення не стосується безпосереднього визнання права на доступ до Інтернету як самостійного конституційного права, воно має значення для розуміння конституційних гарантій реалізації прав людини в цифровому середовищі. На нашу думку, цей підхід підтверджує необхідність забезпечення доступу до інформації з одночасним дотриманням права на приватність і захист персональних даних.

Варто згадати Директиву (ЄС) 2018/1972, якою запроваджено Європейський кодекс електронних комунікацій. Вона передбачає механізми забезпечення універсальних електронних комунікаційних послуг, зокрема належного доступу до Інтернету на доступних для користувачів умовах [10]. Такий підхід свідчить про важливість правових гарантій, які дають змогу людям користуватися сучасними засобами комунікації.

На даний час, для України це питання має особливе значення в умовах воєнного стану, запровадженого 24 лютого 2022 року. Унаслідок збройної агресії Російської Федерації частина громадян опинилася на тимчасово окупованих територіях, де можливості доступу до українських інформаційних ресурсів можуть обмежуватися. Крім того, бойові дії та пошкодження

електронних комунікаційних мереж можуть ускладнювати доступ до Інтернету на окремих територіях. За таких обставин доступ до мережі має значення для отримання важливих повідомлень, підтримання зв'язку з близькими та користування державними електронними послугами.

На нашу думку, право на доступ до Інтернету слід розглядати як право, що має самостійне значення в сучасних умовах, але водночас тісно пов'язане з іншими конституційними правами людини. Відсутність реальної можливості користуватися Інтернетом може істотно ускладнювати здійснення зазначених прав, проте визнання самостійного значення права на доступ до Інтернету не означає автоматичного визнання його окремим конституційним правом у межах чинного законодавства України.

Не менш важливим є захист людей від протиправного контенту в Інтернеті, зокрема висловлювань, спрямованих на розпалювання ворожнечі та дискримінації. В умовах війни це стосується, зокрема, негативного ставлення до внутрішньо переміщених осіб, маніпуляцій щодо соціальної допомоги та працевлаштування, а також використання мовного питання для провокування суспільних конфліктів. При цьому важливо розмежовувати свободу вираження поглядів, яка охоплює критичні думки, та протиправні висловлювання, що становлять підбурювання до дискримінації, ворожнечі або насильства. Правове регулювання має забезпечувати захист людей від таких проявів, не створюючи підстав для свавільної цензури чи необґрунтованого обмеження свободи слова.

Відтак, в умовах інтенсивної цифровізації суспільних відносин право на доступ до Інтернету поступово утверджується як вагома передумова повноцінного здійснення основоположних прав і свобод людини, зокрема права на інформацію, свободи вираження поглядів, права на освіту та участь в управлінні державними справами. Незважаючи на відсутність його

безпосереднього нормативного закріплення як самостійного права в Конституції України, системне тлумачення конституційних положень у взаємозв'язку з міжнародно-правовими стандартами у сфері прав людини дає підстави розглядати доступ до Інтернету як юридично значущу складову реалізації конституційних прав у цифровому середовищі. Вважаємо, що подальше вдосконалення національного законодавства має передбачати формування дієвих правових та інституційних гарантій доступності мережі Інтернет, забезпечення рівності можливостей її використання, належного захисту прав користувачів, а також установлення чітких критеріїв правомірності та пропорційності можливих обмежень доступу. Особливого значення в цьому контексті набуває недопущення цифрової дискримінації та мінімізація ризиків цифрового виключення окремих категорій населення. Послідовне нормативне врегулювання зазначених питань сприятиме зміцненню конституційних гарантій прав і свобод людини, адаптації національної системи їх захисту до сучасних технологічних викликів та забезпеченню належних умов для реалізації правового статусу особи в цифровому суспільстві.

Список використаних джерел

1. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 30 трав. 2026 р. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 11.10.2026).
2. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. Юридичний науковий електронний журнал. 2021. № 10. С. 58–61. URL: <https://doi.org/10.32782/2524-0374/2021-10/12> (дата звернення: 11.10.2026).

3. Марчук М. І. Право на інтернет як базове право людини. 2019. С. 116–119. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/33.pdf (дата звернення: 11.10.2026).
4. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 11.10.2026).
5. Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо використання Посібника з прав людини для Інтернет-користувачів від 16.04.2014. URL: [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805c6f3d%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805c6f3d%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) (дата звернення: 11.10.2026).
6. Case of Ahmet Yıldırım v. Turkey : judgment of the European Court of Human Rights, 18 December 2012, application no. 3111/10. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%226.\tCase%20of%20Ahmet%20Y%24%B1ld%C4%B1r%C4%B1m%20v.%20Turkey%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%2201-115705%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%226.\tCase%20of%20Ahmet%20Y%24%B1ld%C4%B1r%C4%B1m%20v.%20Turkey%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%2201-115705%22]}) (дата звернення: 11.10.2026).
7. Case of Cengiz v. Turkey : judgment of the European Court of Human Rights of 1 December 2015 (Applications nos. 48226/10 and 14027/11). URL: <https://cedem.org.ua/library/yespl-vyznav-blokuvannya-youtube-porushennyam-svobody-slova/> (дата звернення: 11.10.2026).
8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 11.10.2026).

9. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : рішення Конституційного Суду України від 20.01.2012 № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> (дата звернення: 11.10.2026).
10. Директива (ЄС) 2018/1972 Європейського Парламенту і Ради від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text (дата звернення: 11.10.2026).

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.7:004.056.5(477)

БІОМЕТРИЧНІ ДАНІ ЯК ОБ'ЄКТ КОНСТИТУЦІЙНО-ПРАВОВОЇ ОХОРОНИ

Степанова Анастасія Михайлівна,
6 курс, освітня програма «Право»,
юридичний факультет,
Ужгородський університет

В епоху глобальної діджиталізації та стрімкого розвитку систем штучного інтелекту відбувається повсюдне поширення біометричних технологій, які здатні розпізнавати людину дистанційно та мультимодально. На відміну від паролів чи документів, які можна заблокувати або замінити у разі їх компрометації, біометричні характеристики є вродженими та незмінними. Відтак, порушення безпеки таких даних створює велику загрозу для особи. З огляду на це, несанкціонований збір біометрії є не просто порушенням режиму інформаційної безпеки, а прямим посяганням на людську гідність ст. 28 Конституції України та конституційне право на невтручання в особисте і сімейне життя ст. 32 Конституції України [1]. Тому конституційно-правова охорона біометричних даних потребує доктринального осмислення та виокремлення їх у специфічний об'єкт із найвищим рівнем захисту.

На міжнародному рівні біометричні дані визнаються особливою категорією інформації, що вимагає жорсткого регулювання. Загальний регламент ЄС про захист даних (GDPR) відносить їх до «чутливих» персональних даних, визначаючи як інформацію, отриману в результаті спеціальної технічної обробки, що дозволяє унікальну ідентифікацію особи (ст. 9). Аналогічний підхід імплементовано в Конвенції Ради Європи № 108.

В українському нормативному полі базове визначення міститься в Законі України «Про Єдиний державний демографічний реєстр...», де біометрія трактується як сукупність даних, зібраних на основі фіксації стабільних характеристик особи, що істотно відрізняються від параметрів інших осіб [6]. Практика Конституційного Суду України (зокрема, Рішення від 20.01.2012 № 2-рп/2012) недвозначно стверджує, що збирання, зберігання та поширення будь-якої інформації про особу без її згоди є неправомірним втручанням в її особисте життя [2]. Крім того, у знаковому рішенні Верховного Суду (справа № 806/3265/17) було поставлено крапку в питанні неможливості примусового збору біометричних даних під час оформлення паспортів для осіб, які відмовляються від цього через свої переконання [3].

У сучасній доктрині зазначається відсутність єдиного універсального розуміння поняття біометричних даних. Науковці пропонують розмежовувати «біометричні зразки» (сирі дані) та «біометричні шаблони» (машинно-зчитувані моделі), а також поділяти біометрію на фізіологічну (статичну) і поведінкову (динамічну). З позиції конституційного права, біометричні дані слід розглядати не просто як набір ідентифікаторів, а як «цифровий вимір тілесності» людини. Будь-яке втручання у цей простір має підпорядковуватися строгому тесту на пропорційність, закріпленому в практиці ЄСПЛ. Наприклад, у справі «*S. and Marper v. the United Kingdom*» Європейський суд визнав, що безстрокове зберігання біометричних матеріалів осіб, вина яких не доведена, порушує статтю 8 Конвенції про захист прав людини і основоположних свобод [4].

Сучасне українське законодавство залишається розпорошеним та захищає права громадян значно вужче, ніж GDPR чи, наприклад, американський Закон про приватність біометричної інформації (BIPA, штат Іллінойс). Останній є концептуально важливим, оскільки встановлює відповідальність за сам факт

незаконного збору біометрії, не вимагаючи від позивача доведення факту настання матеріальної шкоди (прецедент *Rosenbach v. Six Flags Entertainment Corporation*). У конституційно-правовому вимірі презумпція неправомірності збору біометрії без чітко вираженої згоди має бути абсолютною, а винятки, наприклад, для цілей національної безпеки чи розслідування кримінальних правопорушень - вузько витлумаченими та закріпленими виключно на рівні закону.

Висновки та пропозиції щодо вдосконалення законодавства або правозастосовної практики:

1. Нагальною є потреба ухвалення нової редакції Закону України «Про захист персональних даних», яка б повністю імплементувала стандарти GDPR. Необхідно закріпити поняття біометричних даних у вузькому розумінні, включивши до нього не лише статичні (ДНК, геометрія обличчя, відбитки), а й поведінкові параметри.

2. Доцільно імплементувати в національне законодавство розмежування понять «біометричний ідентифікатор» (унікальна біологічна риса) та «біометричний шаблон» (результат її оцифрування), що усуне прогалини при правовій оцінці роботи систем штучного інтелекту.

3. Українським судам при розгляді спорів щодо захисту персональних даних варто адаптувати доктрину ВІРА, визнаючи, що сам факт несанкціонованого сканування або обробки біометричних характеристик особи (наприклад, системами розпізнавання облич у комерційних закладах) становить самостійне і достатнє порушення статті 32 Конституції України для задоволення позовних вимог без необхідності доведення інших негативних наслідків.

Список використаних джерел

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
2. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>
3. Постанова Великої Палати Верховного Суду від 19.09.2018 у справі № 806/3265/17 (Провадження № 11-460апп18). URL: <https://reyestr.court.gov.ua/Review/76790938>
4. Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04) : Judgment of 04 December 2008 / European Court of Human Rights. URL: <https://hudoc.echr.coe.int/eng?i=001-90051>
5. Гачкевич А. О. Поняття біометричних даних у законодавстві України та іноземних держав. *Вісник Маріупольського державного університету. Серія: Право*. 2025. Вип. 30. С. 16–26. DOI: 10.34079/2518-1319-2025-15-30-16-26.
6. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 № 5492-VI. *Відомості Верховної Ради України*. 2013. № 51. Ст. 716. URL: <https://zakon.rada.gov.ua/laws/show/5492-17#Text>

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.4:004.056(477)

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ КОНСТИТУЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Торчинович Наталія Петрівна,
здобувачка 2 курсу освітньої програми «Право»
Ужгородського університету

Державні реєстри, виборчі процедури, застосунок «Дія», енергетика і зв'язок сьогодні функціонують передусім як інформаційні системи, тому атака на будь-яку з них зачіпає здатність держави виконувати покладені на неї Конституцією функції, і сприймати її лише як технічний збій уже неможливо. Стаття 17 Основного Закону відносить забезпечення інформаційної безпеки до найважливіших функцій держави поряд із захистом суверенітету і територіальної цілісності [1], проте самого терміна «кібербезпека» в Конституції немає. Л. Келло звертає увагу на те, що кіберзброя діє в проміжку між війною і миром і цим змінює природу загроз національній безпеці [2]. Для України ця теза давно має практичний вимір: після атак на енергосистему 2015–2016 рр. і NotPetya 2017 р. ситуація лише загострилася, а з 2022 р. кількість інцидентів, опрацьованих урядовою командою CERT-UA, зросла майже втричі (рис. 1).

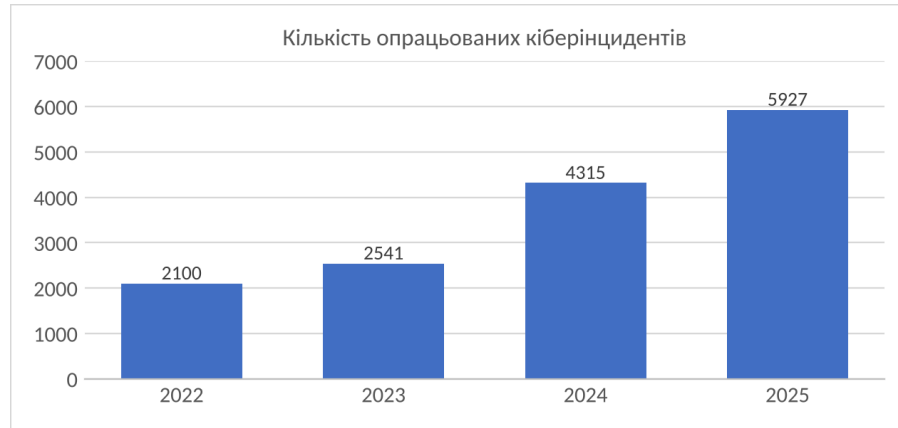


*Рис. 1. Кількість кіберінцидентів, опрацьованих CERT-UA у 2022–2025 рр.
(побудовано автором за даними [3], [4], [5])*

У 2025 р. приріст порівняно з попереднім роком склав 37,4 % [3]. За таких масштабів кібербезпека стосується вже стійкості конституційного ладу. Певною мірою цей зв'язок визнав і законодавець. У Законі «Про основні засади забезпечення кібербезпеки України» до об'єктів кібербезпеки прямо віднесено конституційні права і свободи людини, конституційний лад, суверенітет і територіальну цілісність держави [6]. Закон «Про національну безпеку України» згадує демократичний конституційний лад у визначенні національної безпеки, однак конституційну безпеку як окремий її вид не виділяє [7].

Отже, спеціальний закон конституційний вимір кібербезпеки враховує, тоді як базовий фактично його оминає. Доктрина в цьому питанні пішла далі: О. Лемак обґрунтовує, що конституційна безпека є невід'ємною частиною національної безпеки і означає насамперед захищеність конституційного ладу та самої Конституції [8]. Втім, у вітчизняній літературі конституційна безпека і кібербезпека досі здебільшого досліджуються окремо одна від одної.

Закон № 4336-IX від 27.03.2025 цієї розбіжності не усунув. Ним запроваджено сучасні вимоги до кіберзахисту державних ресурсів і критичної

інформаційної інфраструктури, зокрема обов'язкову посаду керівника з кіберзахисту [9], а українське регулювання наближено до Директиви (ЄС) 2022/2555 (NIS2) [10]. Новели закону мають, однак, переважно організаційно-технічний характер, і питання про межу між кіберзахистом та непропорційним втручанням у права людини в ньому фактично не порушено. Слід зазначити, що NIS2 побудована довкола обов'язків суб'єктів, які надають суттєві та важливі послуги, причому їхнє керівництво несе персональну відповідальність за управління кіберризиками [10]. Європейський законодавець, отже, пов'язує кібербезпеку з належним врядуванням і підзвітністю, і саме цей аспект в українській рецепції поки що відображено найслабше.

Питання меж втручання має і ширший вимір. За висновком М. Данн Кавелті, державоцентрична модель кібербезпеки, за якої мережа використовується для масового стеження, у підсумку знижує захищеність усієї системи, оскільки вразливості, залишені для потреб держави, так само доступні зловмисникам [11]. Конституційний Суд України окремо кібербезпеку не розглядав, проте в Рішенні № 2-рп/2012 зазначив, що інформація про приватне життя особи може поширюватися без її згоди лише у визначених законом випадках і тільки в інтересах національної безпеки, економічного добробуту та прав людини [12]. Найбільш розвинені стандарти в цій сфері напрацьовано практикою ЄСПЛ (табл. 1).

Таблиця 1. Стандарти ЄСПЛ, релевантні для заходів кіберзахисту

Справа	Позиція Суду	Значення для кібербезпеки
Roman Zakharov v. Russia (2015) [13]	Законодавство, що дозволяє перехоплення без попереднього судового контролю, само по собі порушує ст. 8 Конвенції	Доступ до комунікацій з метою кіберзахисту потребує незалежного попереднього контролю
Big Brother Watch and Others v. UK (2021) [14]	Масове перехоплення допустиме, зокрема для протидії кібератакам, але лише з гарантіями на кожному етапі	Легітимна мета не звільняє від процедурних гарантій
Centrum för rättvisa v. Sweden (2021) [15]	Підтверджено підхід «наскрізних гарантій» і вимогу ефективного нагляду	Потрібен постійний зовнішній контроль за спецслужбами
Podchasov v. Russia (2024) [16]	Обов'язок провайдера забезпечити дешифрування порушує ст. 8; шифрування захищає права користувачів	Послаблення шифрування в ім'я безпеки суперечить самій безпеці

Таблиця 1 побудована автором на основі [13] [14] [15] [16]

На необхідності окремих гарантій для інформаційних прав людини в цифровому середовищі наголошують і сучасні українські дослідники [17]. Таким чином, закон, доктрина і судова практика вже пов'язують кібербезпеку з конституційними цінностями, хоча цілісного підходу, який поєднав би ці положення, досі не вироблено.

Як видається, кібербезпеку доцільно розглядати як функціональний елемент конституційної безпеки, конституційна основа якого існує вже сьогодні.

Йдеться про ст. 17 Конституції у поєднанні зі ст. 3, за якою утвердження і забезпечення прав і свобод людини є головним обов'язком держави [1]. На цій підставі пропонується таке визначення: кібербезпека як елемент конституційної безпеки є станом захищеності конституційного ладу, прав і свобод людини та безперервності роботи органів публічної влади в кіберпросторі, за якого заходи кіберзахисту здійснюються лише на підставі, в межах і у спосіб, визначені Конституцією та законами України. Остання частина визначення має принципове значення, оскільки законність заходів захисту тут включено до змісту самого поняття кібербезпеки. Структуру такого розуміння відображено на рис. 2.

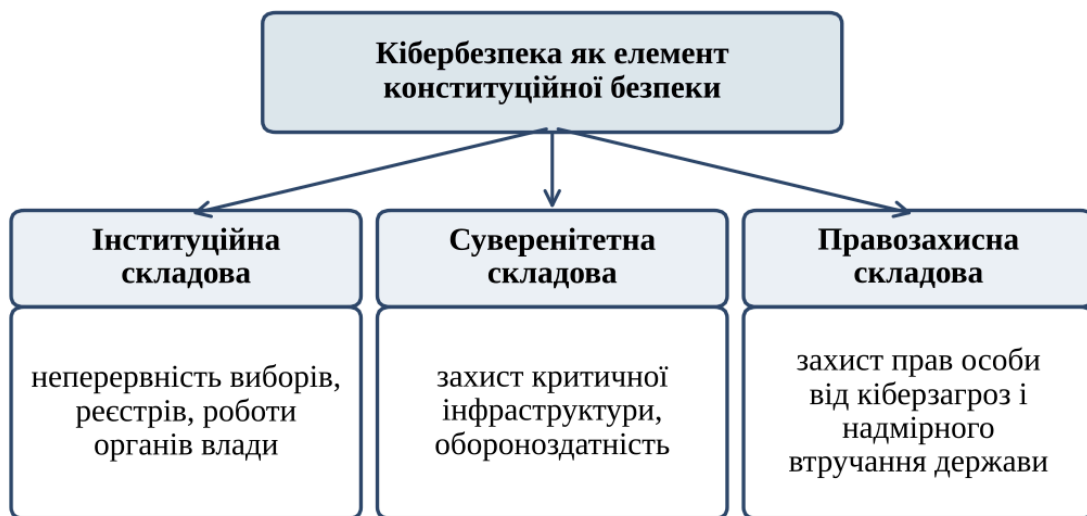


Рис. 2. Конституційний вимір кібербезпеки (розроблено автором на основі [1], [6])

Саме правозахисна складова відрізняє конституційний підхід від суто безпекового. Кібербезпека має подвійну природу: захищаючи конституційний лад, вона водночас може бути використана і на шкоду йому. Моніторинг трафіку, доступ до даних, блокування ресурсів зачіпають права, гарантовані ст.

31, 32 і 34 Конституції, обмеження яких допускається лише у випадках, передбачених самою Конституцією [1]. У зв'язку з цим захід кіберзахисту, що обмежує права особи, має відповідати чотирьом вимогам: законності, легітимності мети, необхідності та підконтрольності незалежному судовому чи парламентському органу. Для прикладу можна взяти блокування сайту, через який поширюється шкідливе програмне забезпечення. Підстави і процедура блокування мають бути встановлені законом, відомчого акта для цього недостатньо; мета є легітимною, якщо йдеться про захист критичної інфраструктури чи даних громадян; блокування всього домену допустиме лише за неможливості обмежитися конкретною сторінкою; власник ресурсу повинен мати змогу оскаржити рішення до суду, а сам захід – переглядатися через визначений строк. Невідповідність хоча б одній із цих вимог робить захід непропорційним.

Окремо варто зупинитися на питанні шифрування. Іноді безпеку держави в мережі пропонують забезпечувати за рахунок безпеки користувачів, з чим погодитися складно. Рішення у справі Podchasov [16] і висновки Данн Кавелті [11] свідчать про те, що держава, послаблюючи шифрування для власних потреб, послаблює насамперед себе. Під час війни це особливо відчутно, бо стійкість держави в кіберпросторі значною мірою залежить від довіри громадян до її цифрових сервісів. Схожа проблема є і в євроінтеграційному аспекті: технічні вимоги права ЄС Україна переймає значно швидше, ніж закладену в ньому логіку підзвітності, хоча саме вона є основою і NIS2, і Cyber Resilience Act, який вимагає забезпечення безпеки цифрових продуктів протягом усього їхнього життєвого циклу [18]. Інструменти міжнародної співпраці в Україні існують давно, адже Конвенцію Ради Європи про кіберзлочинність ратифіковано ще у 2005 р. [19]; бракує передусім конституційно-правового

осмислення проблеми. Щодо доповнення ст. 17 Конституції терміном «кібербезпека», то воно навряд чи є нагальним: чинний текст дає для цього достатню основу, а ст. 157 унеможлиблює зміну Основного Закону в умовах воєнного стану [1].

Отже, кібербезпека є функціональним елементом конституційної безпеки, що ґрунтується на ст. 3 і 17 Конституції; її конституційний вимір охоплює інституційну, суверенітетну і правозахисну складові. Безпека користувачів є передумовою безпеки держави. Чинне законодавство містить неузгодженість між спеціальним і базовим законами та не передбачає механізмів контролю за заходами кіберзахисту, що обмежують права людини. Можливі шляхи усунення цих недоліків наведено в табл. 2.

Таблиця 2. Пропозиції щодо вдосконалення законодавства

Виявлена проблема	Пропозиція	Правова основа
Конституційна безпека не закріплена в базовому законі	Доповнити ст. 1 Закону «Про національну безпеку України» поняттям конституційної безпеки, віднісши кібербезпеку до засобів її забезпечення	Ст. 17, 92 Конституції [1]; [8]
Немає загального правила про межі заходів кіберзахисту	Закріпити в Законі № 2163-VIII тест: законність, легітимна мета, необхідність, підконтрольність	Ст. 64 Конституції [1]; [12]

Виявлена проблема	Пропозиція	Правова основа
Відсутній незалежний контроль за доступом до комунікацій	Запровадити попередній судовий дозвіл і щорічне звітування суб'єктів кібербезпеки перед профільним комітетом Верховної Ради	Ст. 31 Конституції [1]; [13], [14], [15]
Ризик вимог щодо послаблення шифрування	Заборонити покладати на провайдерів загальний обов'язок послаблювати наскрізне шифрування	[16]
Гармонізація з правом ЄС має переважно технічний характер	Переносити принципи підзвітності керівництва та безпеки продуктів протягом життєвого циклу	[10], [18]

Таблиця 2 побудована автором на основі [1] [10] [12] [14] [15] [16] 18]

Запропоновані кроки не потребують зміни Конституції, тож їх можна реалізувати вже зараз. Це дало б змогу використовувати кібербезпеку як інструмент захисту конституційного ладу, що спирається на права людини.

Список використаних джерел

1. Конституція України : від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Kello L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*. 2013. Vol. 38, No. 2. P. 7–40. DOI: https://doi.org/10.1162/ISEC_a_00138
3. Торік CERT-UA опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. Полтавська обласна військова адміністрація. 12.01.2026. URL: <https://poda.gov.ua/news/251006>
4. Поліковська Ю. Урядові кіберфахівці за 2024 рік опрацювали 4315 кіберінцидентів. *MediaSapiens*. 08.01.2025. URL: <https://ms.detector.media/kiberbezpeka/post/37156/2025-01-08-uryadovi-kiberfakhivtsi-za-2024-rik-opratsyuvaly-4315-kiberintsydentiv/>
5. У 2022 році CERT-UA опрацювала понад 2 тис. кібератак на Україну. DOU. URL: <https://dou.ua/lenta/news/hacker-attacks-on-ukraine/>
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
8. Лемак О. В. Значення і роль Конституції в забезпеченні національної безпеки: аспекти сутнісних характеристик. *Аналітично-порівняльне правознавство*. 2024. № 3. С. 69–76. DOI: <https://doi.org/10.24144/2788-6018.2024.03.11>
9. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної

інформаційної інфраструктури : Закон України від 27.03.2025 р. № 4336-IX.
URL: <https://zakon.rada.gov.ua/laws/show/4336-20>

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

11. Dunn Cavelty M. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics. 2014. Vol. 20, No. 3. P. 701–715. DOI: <https://doi.org/10.1007/s11948-014-9551-y>

12. Рішення Конституційного Суду України у справі щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : від 20.01.2012 р. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12>

13. Roman Zakharov v. Russia : judgment of the European Court of Human Rights (Grand Chamber) of 04.12.2015, application no. 47143/06. URL: <https://hudoc.echr.coe.int/eng?i=001-159324>

14. Big Brother Watch and Others v. the United Kingdom : judgment of the European Court of Human Rights (Grand Chamber) of 25.05.2021, applications nos. 58170/13, 62322/14, 24960/15. URL: <https://hudoc.echr.coe.int/eng?i=001-210077>

15. Centrum för rättvisa v. Sweden : judgment of the European Court of Human Rights (Grand Chamber) of 25.05.2021, application no. 35252/08. URL: <https://hudoc.echr.coe.int/eng?i=001-210078>

16. Podchasov v. Russia : judgment of the European Court of Human Rights of 13.02.2024, application no. 33696/19. URL: <https://hudoc.echr.coe.int/eng?i=001-230854>

17. Пирога І. С., Колб О. С. Інформаційні права людини в цифровому просторі. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 89, ч. 1. С. 216–221. DOI: <https://doi.org/10.24144/2307-3322.2025.89.1.29>
18. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union. 2024. L, 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
19. Конвенція про кіберзлочинність : Рада Європи ; від 23.11.2001 р. (ETS No. 185) ; ратифіковано Законом України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК: 347.51:004.8

ЦИВІЛЬНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ: ПІДХОДИ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА

Ухаль Катерина Павлівна,
Ужгородський університет,
студентка юридичного факультету,
ORCID: 0009-0009-5470-3645
kateryna.ukhal@student.uzhnu.edu.ua
м. Ужгород, Україна

Науковий керівник: старший викладач кафедри конституційного права та порівняльного правознавства,
Ужгородський університет,
доктор філософії **Продан Вікторія Іванівна**

Актуальність дослідження є надзвичайно важливим через швидкий розвиток технологій штучного інтелекту, який створює нові завдання для цивільно-правового регулювання. Зокрема, це стосується визначення відповідальних сторін, встановлення причинно-наслідкових зв'язків та компенсації завданої шкоди. Ця тема набуває особливої ваги в контексті створення єдиних підходів до регулювання штучного інтелекту в Європейському Союзі та необхідності вдосконалення українського законодавства з урахуванням європейських стандартів.

Штучний інтелект є технологією, яка здатна аналізувати дані, формувати результати, робити прогнози і в деяких випадках самостійно приймати рішення чи виконувати певні дії. Саме здатність сучасних систем штучного інтелекту діяти з певним рівнем автономії породжує нові виклики для правового

регулювання, особливо у сфері цивільно-правової відповідальності за спричинену шкоду.

Як зазначає колектив авторів, 20 жовтня 2020 року Європейський Парламент затвердив резолюцію, яка містить рекомендації для Комісії щодо правового режиму цивільної відповідальності за заподіяну шкоду системами штучного інтелекту (2020/2014(INL)). У вступній частині цієї резолюції підкреслено, що для максимального використання переваг штучного інтелекту та уникнення можливих зловживань його системами, а також для запобігання регуляторній дезінтеграції в межах Союзу, надзвичайно важливо розробити єдине, принципово орієнтоване та перспективне законодавство, яке діятиме суто на усій території Союзу для всіх систем ШІ. Розвиток технологій не повинен ослаблювати рівень захисту користувачів від можливої шкоди, завданої пристроями та системами, які застосовують штучний інтелект. Визначення відповідальності в разі заподіяння шкоди чи збитків системами штучного інтелекту є одним з ключових аспектів, які потребують вирішення у цих рамках [1 с.153].

Традиційна модель цивільно-правової відповідальності базується на можливості ідентифікації особи, яка своїми діями або бездіяльністю завдала шкоди. Однак, у застосуванні штучного інтелекту ця модель може стати складнішою, оскільки результат роботи такої системи є наслідком взаємодії між розробником, виробником, постачальником, власником або користувачем, а також самою технологією і даними, на яких вона навчалася.

Особливої уваги заслуговують ситуації, коли система штучного інтелекту приймає рішення, що прямо спричиняє негативні наслідки. Наприклад, алгоритмічна помилка може викликати фінансові втрати, неналежне використання персональних даних, пошкодження майна або іншу матеріальну

чи нематеріальну шкоду. У такого роду ситуаціях виникає питання: хто саме має нести відповідальність, розробник системи, її виробник, власник чи безпосередній користувач.

Сам по собі штучний інтелект не здатен здійснювати самостійні рішення, що вказує на те, що відповідальність за потенційну шкоду, спричинену використанням систем або додатків ШІ, несуть окремі особи, організації чи державні утворення. Слід відзначити, що технології ШІ функціонують у межах комплексних систем, що є ключовою відмінністю між системами штучного інтелекту та звичайними комп'ютерними програмами [2 с. 270].

Ідея запровадження відповідальності оператора або власника системи, аналогічно до статті 1187 Цивільного кодексу України, яка врегульовує джерела підвищеної небезпеки, видається логічною, тому що саме оператор фактично контролює рішення щодо експлуатації системи. Такий підхід особливо актуальний для систем, що мають фізичну взаємодію з навколишнім середовищем, таких як автономний транспорт або промислові роботи. Але для надскладних автономних систем контроль може бути лише формальним, знову покладаючи невиправданий ризик на кінцевого користувача чи оператора, який не зміг передбачити або уникнути помилки.

Зважаючи на ці виклики, об'єктивна відповідальність стає необхідною для забезпечення захисту потерпілого навіть тоді, коли вину розробника чи оператора встановити неможливо. Хоча впровадження такої моделі пов'язане з економічними ризиками, змушуючи виробників і операторів ШІ створювати резервні фонди або страхові механізми, що значно збільшує витрати, вона гарантує найвищий рівень компенсації. Саме страхування є ключовою складовою цієї системи, і в країнах ЄС активно розглядається можливість впровадження спеціальних страхових полісів для штучного інтелекту, схожих на

автотранспортні. Це дозволить ефективно розподілити ризики та компенсувати збитки, незалежно від складності технологій, знімаючи частину відповідальності з кінцевих користувачів [3 с. 92-93].

Є нагальною необхідність усвідомлення, що штучний інтелект самотійно не повинен бути автоматично визнаний суб'єктом цивільно-правової відповідальності. Набуття системою ШІ статусу окремого юридичного суб'єкта не вирішує питання компенсації збитків, оскільки ця система не має власного майна і традиційної юридичної волі. Важливо визначити особу, яка здійснює контроль над створенням, впровадженням або використанням даної технології.

При встановленні відповідальної сторони слід враховувати специфіку конкретної ситуації. Якщо шкода виникає через недоліки програмного забезпечення, відповідальність може лежати на розробнику або виробнику. У випадках неправильного налаштування системи або її використання всупереч правилам, відповідальною може бути визнана особа користувача чи оператора. Проте, коли система функціонує автономно і її поведінку складно передбачити, звична модель доведення вини може виявитися недостатньо дієвою.

Тому, Європейський Союз розробляє унікальну регуляторну структуру для управління штучним інтелектом, яку втілює Акт ЄС про штучний інтелект (AI Act). На відміну від традиційних методів, що зазвичай зосереджуються на реакції після виникнення шкоди, європейська модель акцентує увагу на активному запобіганні потенційним ризикам, які можуть виникати під час використання технологій штучного інтелекту.

Архітектура AI Act будується на підході, що орієнтується на ризики, що є спробою досягти оптимального балансу між стимулюванням інновацій та захистом фундаментальних прав, здоров'я і безпеки громадян [4 с. 120].

Для забезпечення сталого та високого рівня захисту суспільних інтересів у сферах здоров'я, безпеки та основних прав людини, необхідно запровадити уніфіковані правила для систем штучного інтелекту з високим рівнем ризику. Ці положення повинні бути вільними від дискримінації та узгоджуватись із міжнародними торговельними зобов'язаннями Союзу. Крім того, вони мають враховувати Європейську декларацію про цифрові права та принципи для Цифрового десятиліття, а також Етичні настанови щодо надійності систем ШІ, розроблені Групою експертів високого рівня з питань штучного інтелекту [5].

AI Act вводить регуляторну систему, засновану на оцінці ризиків, де штучні інтелектуальні системи підпорядковуються різним вимогам відповідно до рівня можливих ризиків. Цей підхід дає змогу накладати суворіші вимоги на системи, що можуть ставити під загрозу права та законні інтереси людей. Він класифікує системи на чотири категорії: неприйнятний ризик, що охоплює заборонені системи, які можуть маніпулювати поведінкою; високий ризик, що потребує суворої сертифікації, зокрема у сферах транспорту та медицини; обмежений ризик, для якого висуваються вимоги до прозорості, наприклад, для чат-ботів; і мінімальний ризик [3 с. 93].

Надзвичайно важливим є визначення чітких обов'язків для розробників, постачальників та користувачів систем штучного інтелекту. Серед іншого, законодавча база повинна містити вимоги щодо управління ризиками, якості даних, технічної документації, прозорості, а також забезпечення контролю та нагляду за функціонуванням цих систем. Це підходить до відповідальності не лише як до результату завданої шкоди, але й як до засобу запобігання її появі.

В Україні на сьогодні відсутній спеціальний комплексний законодавчий акт подібний до AI Act. Регулювання наслідків використання штучного інтелекту відбувається переважно через використання вже існуючих норм

законодавства. Це включає положення Цивільного кодексу України, законодавства про захист персональних даних, інтелектуальну власність, захист прав споживачів та інші нормативно-правові акти.

Цивільний кодекс України окреслює загальні принципи щодо відшкодування як майнової, так і моральної шкоди [6]. Проте ці положення виявляються недостатньо всеосяжними в контексті технологій штучного інтелекту. Ключова проблема полягає у труднощах встановлення причинно-наслідкового зв'язку між діями конкретної особи, роботою алгоритму і завданою шкодою.

У випадках, коли автономна система вчиняє помилку з огляду на специфіку алгоритму, постає питання про те, чи достатньо просто ідентифікувати програмні недоліки, або ж необхідно також довести вину конкретної особи. Встановлення причинного зв'язку в складних системах штучного інтелекту може вимагати глибоких технічних знань та експертного аналізу. Отже, питання цивільної відповідальності за шкоду, спричинену штучним інтелектом, потребує ретельного правового врегулювання на рівні Європейського Союзу. Таке регулювання повинно забезпечувати узгоджену правову визначеність, прозорість та послідовність у застосуванні відповідних норм, що буде на користь громадян, споживачів і бізнесу [7].

На теперішній час українське законодавство не містить комплексного нормативно-правового акту, що систематично регулював би аспекти, пов'язані зі створенням, використанням та функціонуванням штучного інтелекту. Відповідні питання частково покриваються положеннями цивільного законодавства. Однак ці норми не враховують усіх особливостей сучасних систем штучного інтелекту, зокрема їх автономність, здатність до обробки

великих обсягів даних та прийняття рішень без безпосереднього втручання з боку людини.

Регулювання штучного інтелекту в Україні перебуває на етапі становлення та характеризується фрагментарністю нормативної бази. Основним програмним документом у цій сфері є Концепція розвитку штучного інтелекту в Україні, прийнята Кабінетом Міністрів України в 2020 році. У цьому документі визначено стратегічні цілі формування національної системи штучного інтелекту, зазначено напрями державної політики, зокрема щодо етичного використання інтелектуальних систем, розвитку освіти та науки, а також удосконалення нормативно-правової бази. На додаток до Концепції, у 2023 році Міністерство цифрової трансформації України представило Дорожню карту її реалізації, яка заклала основи для створення національних стандартів, механізмів сертифікації та процедур оцінки ризиків систем штучного інтелекту. Ця дорожня карта започатковує регуляторний процес, що включає імплементацію Закону ЄС про штучний інтелект та розробку національного законодавства. Впровадження AI Act є частиною процесу гармонізації українського законодавства з європейськими стандартами у сфері штучного інтелекту та має сприяти правовій інтеграції до ЄС і підвищенню технологічної конкурентоспроможності країни [8 с. 394].

У зв'язку з актуальністю впровадження законодавчої бази щодо штучного інтелекту в Україні, представляється доцільним розробити спеціальний нормативно-правовий акт, який інтегруватиме підходи, прийняті Європейським Союзом, проте буде адаптований під специфіку української правової системи. Цей документ має чітко визначити основні терміни у сфері штучного інтелекту, регулювати правовий статус систем ШІ, а також встановити права та обов'язки осіб, залучених у створення та використання цих систем. Крім того, такі норми

повинні передбачати вимоги щодо безпеки, прозорості та ефективного контролю над функціонуванням системи.

Додатково необхідно комплексно підходити до питання відповідальності за шкоду, яка може бути спричинена експлуатацією систем штучного інтелекту. Законодавчий акт повинен чітко окреслити осіб, які можуть нести відповідальність у разі заподіяння шкоди, включаючи розробників, виробників, постачальників, власників, операторів або користувачів системи. При цьому слід встановити критерії розподілу відповідальності залежно від причин виникнення шкоди, характеру використання системи та рівня контролю, який відповідна особа має над цією системою.

Отже, розвиток штучного інтелекту вимагає суттєвого перегляду традиційних підходів до цивільно-правової відповідальності, особливо в контексті визначення відповідальних осіб, встановлення причинно-наслідкового зв'язку та забезпечення механізмів відшкодування заподіяної шкоди. Однією з ключових позицій є те, що штучний інтелект не слід автоматично розглядати як автономного суб'єкта відповідальності. Натомість необхідно брати до уваги роль і ступінь контролю з боку розробників, виробників, операторів та кінцевих користувачів.

Європейський Союз впроваджує ризик-орієнтовану модель регулювання ШІ, що базується на принципах безпеки та прозорості, акцентуючи увагу на мінімізації потенційних ризиків. В Україні законодавче врегулювання цієї сфери поки залишається фрагментарним, що створює нагальну потребу у вдосконаленні нормативної бази відповідно до європейських стандартів. Основними завданнями мають стати чітке розмежування відповідальності між усіма учасниками правовідносин і формування дієвих механізмів компенсації шкоди. Це сприятиме захисту осіб, які постраждали від дій чи помилок ШІ,

забезпеченню правової визначеності та стимулюватиме відповідальний і безпечний розвиток технологій.

Список використаних джерел

1. Майданик Р. А., Майданик Н. І., Великанова М. М. Відповідальність за шкоду, завдану використанням технологій штучного інтелекту. *Журнал Національної академії правових наук України*. 2021. Т. 28, № 2. С. 150–159. DOI: [https://doi.org/10.37635/jnalsu.28\(2\).2021.150-159](https://doi.org/10.37635/jnalsu.28(2).2021.150-159).
2. Denysiuk S. G., Kononenko V. P. The problem of legal responsibility for the harmful consequences of using artificial intelligence systems. *Ірпінський юридичний часопис*. 2025. Вип. 1 (18). С. 268–279. DOI: [https://doi.org/10.33244/2617-4154.1\(18\).2025.268-279](https://doi.org/10.33244/2617-4154.1(18).2025.268-279)
3. Гнідовський М. С., Сергієнко М. А., Лук'янчиков Б. Є. Правова відповідальність за дії штучного інтелекту: виклики та перспективи регулювання. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 92, ч. 3. С. 90-95 DOI: <https://doi.org/10.24144/2307-3322.2025.92.3.10>
4. Гура М. В. Адаптація законодавства України до норм EU Artificial Intelligence Act: виклики та перспективи. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2025. Вип. 40. С. 119–128 DOI: <https://doi.org/10.26565/2075-1834-2025-40-12>
5. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). *Official Journal of the European Union*. 2018. DOI: <https://doi.org/10.48550/EURLEX.52017IP0051>

6. Цивільний кодекс України : Закон України від 16 січ. 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 17.10.2026).
7. The AI Act Explorer: Regulation (EU) 2024/1689. URL: <https://artificialintelligenceact.eu/ai-act-explorer/> (дата звернення: 17.10.2026).
8. Волосна Я. О. Оптимальні моделі імплементації EU AI Act в українське право з урахуванням ризик-орієнтованого підходу. *Наукові записки Львівського університету бізнесу та права*. Серія економічна. Серія юридична. 2025. Вип. 47. С. 392–399 DOI: <https://doi.org/10.5281/zenodo.18148120>

Дата першого надходження рукопису до видання: 19.10.2026

Дата прийняття до друку рукопису після рецензування: 22.10.2026

Дата публікації: 27.10.2026

УДК 342.4:004.8(477)

КОНСТИТУЦІЙНІ МЕЖІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ОРГАНАМИ ПУБЛІЧНОЇ ВЛАДИ

Фединець Михайло Михайлович,
студент 1 курсу магістратури, освітня програма «Право»,
юридичний факультет,
Ужгородський університет

Цифрова трансформація публічного управління супроводжується дедалі ширшим залученням систем штучного інтелекту (далі - ШІ) до діяльності органів публічної влади: від автоматизованого опрацювання звернень і розгляду адміністративних справ до відеоаналітики, біометричної ідентифікації та оцінювання ризиків. На відміну від приватного суб'єкта, орган публічної влади застосовує ШІ як засіб здійснення владних повноважень, тому помилка, упередженість або непрозорість алгоритму набуває вигляду юридично значущого втручання у права людини. Конституція України [1] не містить положень про ШІ, а спеціального закону в Україні ще не ухвалено, отже межі допустимого використання цієї технології доводиться виводити з конституційних принципів і прав.

На національному рівні регулювання залишається фрагментарним: Закон «Про адміністративну процедуру» [2] започатковує правила розгляду справ в автоматичному режимі, а Закон «Про захист персональних даних» [3] стисло згадує право на захист від автоматизованого рішення, що має правові наслідки. Конституційний Суд України у Рішенні від 20.01.2012 № 2-рп/2012 [4] визнав, що збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою є втручанням в особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в

інтересах національної безпеки, економічного добробуту та прав людини; рішень Конституційного Суду, ухвалених безпосередньо щодо ІІІ, автору не відомо.

У вітчизняній науці утверджується концепція, за якою алгоритмізація не усуває адміністративну дискрецію, а переносить її на етап проєктування системи [5, с. 33]. Досліджуються умови автоматичного вирішення адміністративних справ [6] та інституційні виклики застосування ІІІ в публічному управлінні [7]. Окремо наголошується на ризику «упередження автоматизації», за якого людський контроль стає формальним [5, с. 35], а також на європейських стандартах: праві на належне адміністрування (ст. 41 Хартії основних прав ЄС), праві не підпадати під рішення, засноване виключно на автоматизованому опрацюванні (ст. 22 Регламенту (ЄС) 2016/679), та вимогах до систем ІІІ високого ризику, які використовують публічні органи (Регламент (ЄС) 2024/1689) [5, с. 33]. Проте комплексного конституційно-правового осмислення меж використання ІІІ публічною владою бракує.

Вважаємо, що конституційні межі використання ІІІ органами публічної влади доцільно визначати через чотири взаємопов'язані вимоги, які утворюють своєрідний конституційний тест допустимості.

По-перше, вимога легальності. Відповідно до частини другої статті 19 Конституції [1] органи влади діють лише на підставі, в межах повноважень і у спосіб, що передбачені Конституцією та законами. Отже, запровадження ІІІ потребує закону, який визначає мету, сферу застосування, категорії даних і відповідальний орган; підзаконний акт чи рішення про закупівлю цього не замінюють. Якщо ж ІІІ втручається в право на приватне життя (ст. 32), таке втручання допустиме лише у випадках, визначених законом, і в легітимних інтересах, названих Конституційним Судом [4].

По-друге, вимога пропорційності та неприпустимості звуження прав. Стаття 22 Конституції забороняє звужувати зміст і обсяг наявних прав, а частина друга статті 64 не допускає обмеження, зокрема, рівності перед законом (ст. 24) і права на судовий захист (ст. 55) навіть в умовах воєнного чи надзвичайного стану [1]. Тому безпековий контекст воєнного стану не виправдовує ні алгоритмічної дискримінації, ні позбавлення особи можливості оскаржити автоматизоване рішення. Вимога пропорційності, закріплена в частині другій статті 2 Кодексу адміністративного судочинства [8], має поширюватися й на рішення, підготовлені за допомогою ШІ.

По-третє, вимога людиноцентричності та збереження владного розсуду за людиною. Повноваження належать органам та посадовій особі, а не алгоритму (статті 6, 19), а правосуддя здійснюється виключно судами (ст. 124) [1]. Тому ШІ може бути допоміжним інструментом, але не носієм дискреції чи судової функції. Повна автоматизація припустима лише у формалізованих провадженнях, де результат прямо впливає з достовірних даних і чітких нормативних критеріїв; справи, які потребують оцінювання пропорційності, вразливості особи або балансу приватного та публічного інтересів, вимагають змістовного людського контролю [5, с. 39-40]. Формальне «затвердження» результату роботи алгоритму таким контролем не є [5, с. 35].

По-четверте, вимога прозорості, мотивування та ефективного захисту. Право на судовий захист (ст. 55) і право на відшкодування шкоди, завданої незаконними рішеннями органів влади (ст. 56) [1], передбачають, що особа знає про застосування ШІ, розуміє основні чинники рішення та може його оскаржити [6]. Відповідальність за законність акта має залишатися за органом незалежно від того, розробив він систему самостійно чи придбав у приватного постачальника [5, с. 40].

Конституційно-правові засади використання технологій штучного інтелекту органами публічної влади формуються на основі сукупності положень Конституції України, які, попри відсутність безпосереднього нормативного регулювання відповідних технологій, визначають фундаментальні вимоги до здійснення публічно-владних повноважень. Зокрема, системне тлумачення статей 6, 8, 19, 22, 24, 32, 55, 56, 64 та 124 Основного Закону України дає підстави обґрунтувати конституційні межі впровадження алгоритмічних систем у діяльність органів державної влади та місцевого самоврядування. Визначальним у цьому контексті є формування належних правових умов його застосування, заснованих на принципах верховенства права, законності, юридичної визначеності, пропорційності, недискримінації, прозорості та підзвітності публічної адміністрації. При цьому використання інтелектуальних алгоритмічних систем не повинно призводити до фактичного делегування їм владних повноважень, усунення уповноваженої посадової особи від здійснення адміністративного розсуду чи нівелювання юридичної відповідальності відповідного суб'єкта владних повноважень за ухвалені рішення.

З огляду на зазначене, вбачаємо за доцільне комплексне нормативне врегулювання використання штучного інтелекту у сфері публічного управління з урахуванням європейських стандартів захисту основоположних прав людини. Зокрема, у разі прийняття спеціального законодавчого акта у сфері штучного інтелекту доцільно передбачити окремий комплекс положень, присвячених особливостям його застосування органами публічної влади, із визначенням допустимих сфер використання, правових підстав, процедурних обмежень та гарантій людського контролю. Особливого нормативного врегулювання потребує недопущення ухвалення виключно автоматизованих індивідуальних владних рішень у випадках, коли законодавство передбачає здійснення

адміністративного розсуду, індивідуальну оцінку обставин справи або застосування оціночних правових категорій. Поряд із зазначеним, обґрунтованим видається запровадження обов'язкової попередньої оцінки впливу систем штучного інтелекту на основоположні права і свободи людини, а також формування публічного реєстру відповідних систем, які використовуються органами державної влади та місцевого самоврядування, з урахуванням законодавчо визначених обмежень щодо розкриття інформації.

Список використаних джерел

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 11.10.2026).
2. Про адміністративну процедуру : Закон України від 17 лют. 2022 р. № 2073-IX. URL: <https://zakon.rada.gov.ua/laws/show/2073-20#Text> (дата звернення: 11.10.2026).
3. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 11.10.2026).
4. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січ. 2012 р. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12> (дата звернення: 11.10.2026).
5. Сірко В. С. Адміністративна процедура в умовах алгоритмізації публічного адміністрування: межі дискреції, гарантії прав людини та стандарти

Європейського Союзу. *Forum Prava*. 2026. Т. 87, № 3. С. 31-43. DOI: <https://doi.org/10.32631/fp.2026.3.04>. (дата звернення: 11.10.2026).

6. Хлібороб Н. Є. Розгляд та вирішення адміністративних справ в автоматичному режимі у світлі Закону України «Про адміністративну процедуру». *Проблеми законності*. 2023. Вип. 163. С. 267-279. DOI: <https://doi.org/10.21564/2414-990X.163.292387>. (дата звернення: 11.10.2026).

7. Костенко І. В. Штучний інтелект у системі публічного управління: інституційні виклики, управлінські трансформації та нормативно-правові орієнтири. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 92, ч. 3. С. 206-212. DOI: <https://doi.org/10.24144/2307-3322.2025.92.3.27>. (дата звернення: 11.10.2026).

8. Кодекс адміністративного судочинства України від 6 лип. 2005 р. № 2747-IV. URL: <https://zakon.rada.gov.ua/laws/show/2747-15> (дата звернення: 11.10.2026).

Дата першого надходження рукопису до видання: 12.10.2026

Дата прийняття до друку рукопису після рецензування: 14.10.2026

Дата публікації: 27.10.2026

УДК 342.8:004.8

ВПЛИВ АВТОМАТИЗОВАНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ НА ВИБОРЧИЙ ПРОЦЕС

Щерба Олександр Сергійович,
студент юридичного факультету,
Ужгородського університету,
м. Ужгород, Україна

email: oleksandr.shcherba@student.uzhnu.edu.ua

Науковий керівник: старший викладач кафедри
конституційного права та порівняльного правознавства
Ужгородського університету,
доктор філософії **Продан Вікторія Іванівна**

Стрімкий розвиток систем штучного інтелекту останнім часом докорінно змінив політичну комунікацію. Якщо в попередні десятиліття під час виборчих кампаній ключовим інструментом цифрового маркетингу був відносно простий мікротаргетинг, то зараз виборчі процеси зазнають впливу автоматизованих систем масового впливу. Генеративні мовні моделі та технології синтетичних медіа дозволяють створювати унікальний, персоналізований контент у великих обсягах з мінімальними витратами.

ШІ може різно впливати на виборчу кампанію та її результати. Це може включати різні способи, як автоматизований аналіз даних виборців, прогнозування політичних настроїв, мікротаргетинг виборців, автоматизовану генерацію виборчої реклами та розповсюдження політичних повідомлень через соціальні мережі.

Використання штучного інтелекту для автоматизації аналізу виборчих даних та прогнозування політичних настроїв ґрунтується на алгоритмах

машинного навчання та статистичних методах, що здатні обробляти значні обсяги інформації. Ці інструменти дозволяють виявляти ключові тенденції, рівень суспільної активності та географічний розподіл голосів, формуючи чітке уявлення про поточний політичний ландшафт. Крім того, аналіз цифрових слідів у соціальних мережах, медіапросторі та публічних виступах політиків дозволяє штучному інтелекту виявляти приховані зв'язки між різними факторами. Це відкриває можливість моделювати динаміку суспільних настроїв і з високою точністю передбачати майбутню виборчу активність у реальному часі [1, с. 19].

Сучасні алгоритми штучного інтелекту можуть досліджувати детальні цифрові сліди користувачів у соціальних мережах, за допомогою яких вони виявляють приховані страхи, тривоги та політичні схильності. Використовуючи цю інформацію, ШІ автоматично генерує персоналізовані психологічні тригери.

Алгоритми штучного інтелекту аналізують великі масиви даних про поведінку користувачів в Інтернеті, що дає змогу формувати комплексні цифрові профілі виборців. Ці профілі базуються на їхній активності в соціальних мережах, звичках купівлі товарів, споживанні контенту та інших онлайн діях. У такому контексті політичні кампанії здатні не лише прогнозувати тип інформації, яку виборці бажають отримати, але й визначати найбільш ефективний час і формат її подачі. Це полегшує автоматизацію процесів збору даних та створення персоналізованих повідомлень, які можуть спрямовуватися на вразливі аспекти переконань або підсилювати вже існуючі політичні вподобання та прихильності [2, с. 132].

Технологія електоральних маніпуляцій за допомогою штучного інтелекту є складним багатоступеневим процесом, що функціонує як кібернетичний конвеєр. Він базується на постійному зборі даних, автоматичному створенні

контенту та розповсюдженні інформації через алгоритми. Весь процес починається з етапу аналізу великих даних, під час якого алгоритми машинного навчання обробляють цифрові відомості про користувачів соціальних мереж, історію їхніх пошукових запитів та геолокаційні метадані. Цей етап спрямований на психометричне профілювання електорату. Використовуючи моделі типу OCEAN, штучний інтелект поділяє виборців на безліч мікрогруп (кластерів) відповідно до їхніх провідних психотипів, визначаючи приховані страхи, політичні упередження та рівень тривожності.

Зокрема, застосування психографії – аналізу психологічних характеристик виборців – дозволяє створювати повідомлення, які допомагають налаштовувати певний емоційний стан або політичну орієнтацію індивіда. Це може охоплювати все, починаючи від спеціально пристосованих політичних рекламних оголошень до цілеспрямованого поширення фейкових новин, що підсилюють певні емоції чи страхи [3, с. 167].

З цієї причини постає питання, яке полягає у регулюванні таких технологій, для того, щоб не допустити зловживання ними і захистити право громадян на справедливий вибір. Перехід від традиційних виборчих методів до цифрових технологій створює нові можливості для політичних маніпуляцій, але й ставить перед суспільством складні етичні питання.

Штучний інтелект має величезний потенціал для зміни політичних стратегій, але також створює нові загрози для демократичних принципів проведення виборів. Одним із таких викликів є використання технологій ШІ для поширення неправдивих новин та дезінформації, що може не тільки впливати на політичні погляди виборців, а й суттєво підірвати довіру до виборчої системи в цілому.

Швидке створення контенту за допомогою алгоритмів штучного інтелекту, який може виглядати повністю правдоподібно, навіть якщо це лише вигадка, відкриває чимало можливостей для маніпулювання інформацією. Це явище, відоме як «інформаційне втручання», набуває все більшого поширення, особливо в контексті політичних кампаній. Штучний інтелект використовується для розробки та поширення фальшивих новин і маніпуляційних матеріалів, що можуть загрожувати політичній стабільності [2, с. 132].

На ключовій стадії технологічних маніпуляцій відбувається створення так званих ефектів ехокамер, де виборці отримують тільки ту інформацію, що зміцнює їхні власні переконання. Штучний інтелект, використовуючи алгоритми таргетингу, генерує емоційно насичені повідомлення, базуючись на особистих вподобаннях користувачів і їхній попередній взаємодії з контентом. Це нагнітає ілюзію належності до певної політичної ніші, де подається лише узгоджена з їхнім світоглядом інформація, в той час як альтернативні думки виключаються або відкидаються. Така ситуація не лише ускладнює ведення конструктивного політичного діалогу, але й сприяє суспільній поляризації. Одночасно це впливає і на виборчі результати через маніпуляції з даними, що можуть призводити до зміщення голосів або навіть фальсифікацій [4, с. 188].

Один із найбільш найяскравіших інцидентів, що демонструють вплив штучного інтелекту та кібератак на президентські вибори 2016 року в Сполучених Штатах Америки, полягав у широко розповсюджених припущеннях про причетність російських хакерів під час виборчої кампанії. Представники Демократичної партії офіційно заявили, що стали об'єктами кібератак. Згодом таємний звіт Центрального розвідувального управління підтвердив, що інциденти були організовані російськими операторами з метою підтримки Дональда Трампа в його прагненні до номінації від Республіканської

партії та зрештою обрання на посаду президента. Обрання Трампа інтерпретувалося багатьма як сприятливе для російських геополітичних інтересів завдяки його позиції щодо більш ізольованої та менш інтервенціоністської зовнішньої політики США. Під час передвиборчої кампанії Трамп висловлював намір зменшити зобов'язання США перед НАТО та уникати втручання у справи, що стосуються України та Криму. Таким чином, перемога Трампа стала потенційним викликом для традиційних принципів зовнішньої політики США, включаючи глобальне просування демократії та американських цінностей, як зазначено в Парламентській асамблеї Середземномор'я. Кампанія дезінформації, організована росією під час виборів 2016 року, виразно продемонструвала силу кібервійни та цифрових форм дезінформації для впливу на політичні результати – це досягається шляхом методів, які були б значно менш ефективними при використанні традиційних військових засобів, таких як вторгнення чи бомбардування. Російські оперативники використовували передові технології у межах чітко скоординованої стратегії маніпулювання громадською думкою та підриву демократичних процесів [5].

На нашу думку, серед розмаїття гібридних загроз найнебезпечніше місце посідають технології синтетичних медіа, зокрема діпфейки, які дозволяють із високим ступенем реалістичності фальсифікувати аудіо- та відеоматеріали за участю політичних акторів. Подібні дезінформаційні кампанії спрямовані на навмисне викривлення інформаційного простору, дискредитацію опонентів та дезорієнтацію виборців у критичні моменти електорального циклу, коли спростування фейку в стислі терміни є практично неможливим. Внаслідок цього штучно створений контент перетворюється на ефективну зброю когнітивної війни, здатну безпосередньо впливати на результати голосування та підривати суспільну довіру до інституту виборів загалом.

Прикладом застосування технології Deepfake на виборах став інцидент у Словаччині. За два дні до виборів на Facebook з'явився аудіозапис, на якому двоє людей обговорюють можливі способи фальсифікації виборів, зокрема через купівлю голосів у ромської меншини. Один із голосів нібито належав лідеру партії «Прогресивна Словаччина» Міхалу Шимечці, а інший – Моніці Тодовій з газети Denník N. Обидві сторони заявили, що запис є фейком, але його поява мала значний вплив, адже це сталося під час 48-годинного періоду тиші в медіа та політиці, що ускладнило його спростування. Згодом з'ясувалося, що запис створено за допомогою нейронної мережі.

У сучасному науковому дискурсі, що стосується впливу генеративного штучного інтелекту на електоральні процеси, виокремилися два основних підходи: технопесимістичний та помірковано-оптимістичний. Емпіричні спроби верифікації цих гіпотез продемонстрували неоднозначні результати, що зокрема підтверджується експериментами, проведеними дослідниками з Корнельського університету, а також висновками Інституту Алана Тюрінга.

Професори Корнельського університету, Сара Крепс і Даг Крінер, розіслали тисячі електронних листів більш ніж 7 тисячам представників штатів. У листах імітувалися запити від занепокоєних виборців, причому половина з них була згенерована штучним інтелектом. Експеримент довів, що за допомогою ШІ можна створити фіктивні запити, які можуть заплутати передвиборчий штаб кандидата. Ці тексти, завдяки технології машинного навчання, важко відрізнити від написаних людьми. Водночас оптимістичними є висновки авторитетного британського Інституту Алана Тюрінга. Проаналізувавши понад 100 національних виборів з 2023 року, дослідники виявили, що втручання ШІ відбулося лише в 19 випадках. До того ж докази не

показали жодних явних змін у результатах виборів порівняно з очікуваними показниками кандидатів згідно з опитуваннями [6, с. 28].

Є і позитивний вплив ІІІ на виборчий процес, а саме через забезпечення скорочення впливу людського фактору на процедури ведення списків виборців, інформування виборців про перебіг передвиборної кампанії, авторизації виборців, навчання членів виборчих комісій, забезпечення кібербезпеки і протидії шахрайству у виборчому процесі та електронне голосування може принести користь із забезпечення принципу прозорості під час виборів. Сучасні технології впливають на те, як організовуються та проводяться виборчі кампанії. Від традиційних засобів масової інформації, таких як радіо, телебачення та кіно, до цифрових платформ, технологічна еволюція уможливила більшу персоналізацію та ефективність політичної комунікації. ІІІ полегшує аналіз великих обсягів даних, роблячи можливими високопрофесійні та персоналізовані кампанії [6, с. 26].

Особливої гостроти у контексті ІІІ-маніпуляцій набуває теоретичний аспект, який визначається як феномен «ілюзорної легітимності». Це специфічний стан, за якого органи влади бездоганно дотримуються формальної «букви закону» та виборчого регламенту (легальність), але їхні дії та рішення позбавлені реальної суспільної підтримки й морального виправдання через попереднє викривлення електорального поля.

Технології генеративного ІІІ виступають головним каталізатором цього процесу. Формально виборчий процес може виглядати цілком легальним (бюлетені друкуються за стандартом, дільниці відкриваються вчасно), проте використання прихованих алгоритмів мікротаргетингу, діпфейків та автоматизованих бот-мереж знищує реальну політичну конкуренцію ще до початку голосування. Як наслідок, ІІІ дозволяє маніпулювати правосвідомістю

громадян, створюючи вид демократичних процедур, що призводить до глибокої інституційної кризи, падіння довіри після виборів та тотального зниження загальної правової культури суспільства [7, с. 40].

Основними аспектами, які потребують врегулювання є:

1) Керівні принципи «Добросовісного використання ШІ» та добровільні угоди для політичних партій та виробників контенту для їхніх кампаній:

Рекомендації повинні зобов'язувати до чіткого маркування всіх виборчих матеріалів, створених за допомогою штучного інтелекту, а також до впровадження ідентифікаторів, що вказують на джерело контенту. Всі ці обов'язки мають поширюватися також на треті сторони, які займаються створенням контенту від імені політичних партій.

2) Підтримка ЗМІ щодо звітності про загрози за допомогою штучного інтелекту:

У рекомендаціях повинні бути представлені сертифіковані інструменти для виявлення діпфейків, які можуть використовувати медіаорганізації для перевірки контенту. Також слід передбачити механізми для звітування про джерела фейкових новин, створених штучним інтелектом, що допоможе регуляторам у блокуванні відомих сайтів.

3) Уточнення щодо звітності щодо інцидентів зі штучним інтелектом у день виборів:

Потрібно повідомляти про інциденти, пов'язані зі штучним інтелектом, під час дня виборів. Це допоможе уникнути плутанини щодо того, як реагувати на будь-які загрози, пов'язані зі штучним інтелектом, що виникають у критичний період виборчого процесу.

4) Кампанії з підвищення обізнаності громадськості щодо загроз ШІ на виборах:

Виборча комісія має гарантувати, що будь-яка майбутня інформація для виборців містить рекомендації щодо безпеки від загроз, пов'язаних із штучним інтелектом на виборах. Важливо надати поради, як виявити контент, створений за допомогою штучного інтелекту, а також вказати авторитетні органи, до яких можна звертатися за порадою. Крім того, слід інформувати про ризики отримання даних з опитувань через чат-боти на основі штучного інтелекту [8].

Враховуючи євроінтеграційний курс України імплементація норм *AI Act* є надзвичайно актуальною, адже критично важливою є для забезпечення когнітивної безпеки електорального простору, оскільки вона переносить регуляторний тягар безпосередньо на розробників базових генеративних систем. Такий публічно-правовий підхід дозволяє вимагати від технологічних гігантів структурної прозорості, обов'язкового тестування моделей на схильність до дезінформації та чіткої верифікації походження даних. Для держав, які перебувають на етапі цифрової трансформації, адаптація цих європейських орієнтирів є надійним бар'єром проти зовнішнього алгоритмічного втручання та неконтрольованого поширення неправдивих наративів під час виборчих кампаній.

Вирішальне значення для юридичної практики має судова практика. Рішення Конституційного Суду Румунії від 6 грудня 2024 року стало визначальним у світовій практиці конституційного судочинства, оскільки воно скасувало результати першого туру президентських виборів. Суд дійшов висновку про систематичне викривлення виборчого процесу через скоординовану гібридну операцію, в якій ключову роль відіграли алгоритми штучного інтелекту. Згідно з розсекреченими даними розвідки, які використовував Суд, в інформаційному просторі, особливо на платформі TikTok, діяла мережа з понад 25 000 бот-акаунтів, які управлялися

автоматизованими системами. Ці алгоритми не лише штучно підвищували популярність одного з кандидатів, але й застосовували технології мікротаргетингу для обходу правил фінансування кампаній. Суд визнав це втручання порушенням конституційного принципу чесних виборів і суверенного волевиявлення народу, створивши перший у світі правовий прецедент, коли технологічні маніпуляції стали підставою для повного скасування виборчого процесу [9].

Отже, через процеси цифровізації вплив штучного інтелекту на виборчий процес є невідворотним. Але найчастіше вибори зазнають негативного впливу, через різні способи, а саме: автоматизований аналіз даних виборців, прогнозування політичних настроїв, мікротаргетинг виборців, автоматизовану генерацію виборчої реклами та розповсюдження політичних повідомлень через соціальні мережі.

Перша серйозна проблема – це повна втрата довіри до інформації. Сьогодні генеративний ШІ здатний створювати підроблені відео, аудіо та тексти такої якості, що їх неможливо відрізнити від справжніх. Поширення дипфейків набуло надзвичайного поширення. Політики, у свою чергу, тепер можуть легко оголосити будь-який справжній компромат проти себе звичайною роботою штучного інтелекту. Коли суспільство втрачає чіткий орієнтир, де правда, а де брехня, свідомий вибір стає практично неможливим.

Другий важливий аспект – це індивідуальна робота з кожним виборцем за допомогою алгоритмів. Аналізуючи лайки, коментарі та пошукові запити, ШІ допомагає політичним штабам знаходити точкові вразливості кожної людини. Замість загальних передвиборчих програм люди бачать у своїх стрічках новин персоналізований контент. Це розділяє суспільство на ізольовані групи, які

живуть у абсолютно різних інформаційних реальностях і втрачають здатність чути один одного.

Зрештою, виборчий процес дедалі більше залежить від фінансових та технічних можливостей ІТ-центрів. Перевагу отримує той, чиї алгоритми краще прорахували поведінку людини та точніше на неї вплинули. Це ставить під загрозу сам принцип чесних виборів, адже рішення людей стає результатом тонкого математичного моделювання, а не особистих переконань.

Список використаних джерел

1. Асірян С. Р. Використання штучного інтелекту під час виборів, практика, загрози виборчому праву громадян та шляхи подолання. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 77, ч. 2. С. 17–22. doi: <https://doi.org/10.24144/2307-3322.2023.77.2.2>
2. Лазарович М. В., Гончарук-Чолач Т. В., Докаш О. Ю. Штучний інтелект у політичних маніпуляціях та трансформація виборчої культури. *Політикус : науковий журнал*. Серія: Політична культура та ідеологія. 2025. Вип. 1. С. 131–135. DOI: <https://doi.org/10.24195/2414-9616.2025-1.20>
3. Rid Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Profile Books, 2020. 448 p
4. Vianelli Donata, Pegan Giovanna, Patriziade Luca. *International Marketing Strategy: The Country of Origin Effect on Decision-Making in Practice*. Springer, 2020.
5. Ibrahim Nourhan Tosson, Attia Nada Adel. The impact of disinformation generated by AI on democracy case studies: the US presidential elections in 2016 & 2024. *Review of Economics and Political Science*. 2025. Vol. 11, iss. 3. DOI: <https://doi.org/10.1108/REPS-12-2024-0104>

6. Павшук К. О. «Усміхнися і проголосуй»: чи викликає довіру використання штучного інтелекту на виборах? *Проблеми законності : науковий журнал*. 2025. Вип. 169. С. 20–36. DOI: <https://doi.org/10.21564/2414-990X.169.328486>
7. Щерба О. С. Правова культура в контексті легітимації державної влади. *Аналітично-порівняльне правознавство : електронне наукове фахове видання*. 2026. № 4. С. 38–43. DOI: <https://doi.org/10.24144/2788-6018.2026.04.5>
8. AI-Enabled Influence Operations: The Threat to the UK General Election : CETaS Briefing Paper / Sam Stockwell, Megan Hughes, Phil Swatton, Katie Bishop. Centre for Emerging Technology and Security (CETaS), The Alan Turing Institute, 2024. URL: <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-uk-general-election> (дата звернення: 17.10.2026).
9. Hotărârea nr. 32 din 6 decembrie 2024 privind anularea procesului electoral cu privire la alegerea Președintelui României din anul 2024 / Curtea Constituțională a României // Monitorul Oficial al României. Partea I. 2024. Nr. 1231. URL: https://www.ccr.ro/wp-content/uploads/2024/12/Hotarare_32_2024.pdf (дата звернення: 17.10.2026).

Дата першого надходження рукопису до видання: 19.10.2026

Дата прийняття до друку рукопису після рецензування: 22.10.2026

Дата публікації: 27.10.2026

СЕКЦІЯ 14. ПЕДАГОГІЧНІ НАУКИ**UDC 373.5.016:67/68****THEORETICAL FOUNDATIONS OF DEVELOPING TECHNOLOGICAL
COMPETENCIES IN LOWER SECONDARY SCHOOL STUDENTS****Volodymyr Kashuba**

Department of Theory and Methods of Technological Education
Poltava V. G. Korolenko National Pedagogical University
kashubavv85@gmail.com

The transformation of contemporary society, rapid technological development, and the increasing complexity of professional and everyday environments require secondary education to focus not only on the acquisition of subject knowledge but also on the development of students' ability to apply this knowledge in meaningful practical contexts. In this regard, technological competence becomes an important component of the educational outcomes of lower secondary school students, as it determines their capacity to understand technological processes, use tools and materials purposefully, design solutions, solve practical problems, and evaluate the results of their own activities.

The theoretical interpretation of technological competence is closely related to the modern understanding of competence as an integrated combination of knowledge, skills, attitudes and values that enables an individual to act effectively and responsibly in different contexts. UNESCO-IBE emphasizes that competence should not be reduced to a fixed set of skills; rather, it represents a developmental capacity to mobilize knowledge, skills, values and attitudes for meaningful action in changing contexts [1]. This conceptual position is particularly relevant to technological

education, where the learner must continuously combine theoretical understanding with practical action.

Technological competence can therefore be conceptualized as an integrative personal capacity that encompasses technological knowledge, procedural and practical skills, design and engineering thinking, creativity, problem-solving, digital literacy, communication and collaboration, as well as the ability to make informed decisions regarding technological processes and products. Such an interpretation shifts the emphasis from reproductive acquisition of technological information towards the learner's ability to independently design, create, test, improve and evaluate technological solutions.

A significant theoretical basis for this interpretation is provided by the competency-based approach, which changes the logic of educational outcomes. Within this approach, the effectiveness of technological education is determined not only by what students know but also by how effectively they can mobilize their knowledge and skills to address authentic problems. OECD research conceptualizes competence as a combination of knowledge, skills, attitudes and values, emphasizing their interdependence in the development of learners' capacity for responsible action [2]. Consequently, technological competence should be viewed as a dynamic educational outcome rather than a fixed collection of technical skills.

The activity-oriented approach provides another important theoretical foundation. Technological competence develops most effectively through purposeful practical activity in which students become active subjects of the educational process. Designing, modelling, constructing, experimenting, testing materials, operating tools, analysing technological processes and improving products create conditions for the transition from theoretical understanding to practical application. Procedural and technical knowledge are especially important in STEM-oriented education because

they allow learners to investigate phenomena, work with data and apply scientific and technological principles in practical contexts [3].

The project-based approach has particular significance for the formation of technological competence. Project activity integrates goal setting, problem identification, information search, planning, designing, modelling, implementation, testing, reflection and presentation of results. Such a sequence corresponds to the logic of real technological processes and promotes the development of learner autonomy, creativity, responsibility and collaborative skills. The project becomes not simply a final educational product but a structured environment in which students acquire experience of technological decision-making.

Theoretical foundations of technological competence are also strengthened by the principles of STEM and STEAM education. Contemporary European research demonstrates that integrated STEM approaches increasingly focus on creativity, problem-solving, interdisciplinary knowledge and the practical application of science, technology, engineering and mathematics [3]. The 2026 European Commission study on STEM education further emphasizes the importance of STEM competences across primary, secondary and vocational education and analyses approaches that combine STEM with creativity and the arts [4]. Thus, technological education can be interpreted as an important component of an interdisciplinary STEM-oriented learning environment.

An essential characteristic of technological competence is technological thinking. It involves the ability to identify a practical problem, analyse its conditions, generate possible solutions, select appropriate materials, tools and technologies, predict consequences, construct a prototype or model, test the proposed solution and improve it based on the obtained results. This logic is closely connected with engineering design and design thinking, where the process is iterative rather than

linear. The learner therefore acquires not only a technological operation but also a way of thinking oriented towards creating and improving solutions.

The development of technological competence is closely associated with creative and critical thinking. Technological activity requires students to generate alternative ideas, compare possible solutions, assess their feasibility and justify decisions. OECD research on creative thinking demonstrates the importance of students' ability to generate, evaluate and improve ideas, particularly in contexts involving problem solving and the design of solutions [5]. Consequently, technological education provides a favourable environment for the development of creativity through practical experimentation and purposeful transformation of ideas into tangible or digital products.

A modern theoretical model of technological competence should also incorporate digital competence as a complementary component. Contemporary technological processes increasingly involve digital modelling, information search, programming, digital fabrication, simulation, data processing and collaborative online environments. The European Digital Competence Framework DigComp 3.0 emphasizes that digital competence includes not only technical skills but also knowledge, attitudes, responsible behaviour, critical evaluation of information and the ability to use digital technologies purposefully [6]. Therefore, digital tools should be considered not as an independent goal but as instruments that expand students' technological and design capabilities.

An important theoretical principle is interdisciplinarity. Technological problems rarely belong exclusively to one subject domain. Their solution may require mathematical calculations, scientific knowledge, digital tools, artistic and aesthetic decisions, communication skills and an understanding of environmental or social contexts. Contemporary European STEM policy consequently promotes greater

integration between scientific, technological, engineering and mathematical learning, while also emphasizing creativity and interdisciplinary connections [3; 4]. Such integration contributes to the development of a holistic technological worldview.

The effectiveness of technological competence formation also depends on the organization of the educational environment. It should provide opportunities for experimentation, hands-on learning, project work, collaborative problem solving and access to relevant technological resources. At the same time, the use of technology in education should remain pedagogically purposeful: European research indicates that the impact of digital technologies depends substantially on the educational context, instructional design and ways in which technologies are integrated into learning activities [7]. Thus, technological competence cannot be developed merely through increased access to digital devices; it requires meaningful educational scenarios and purposeful practical activity.

Another important theoretical dimension is assessment. Traditional assessment focused predominantly on the reproduction of knowledge does not fully reflect the complexity of technological competence. More appropriate are formative and performance-based approaches that evaluate not only the final product but also the process of problem identification, planning, choice of materials and tools, design decisions, experimentation, ability to overcome difficulties, collaboration, reflection and improvement of the result. Such assessment supports the development of learner agency and makes technological progress visible throughout the educational process.

The theoretical analysis demonstrates that the formation of technological competencies in lower secondary school students should be understood as a multidimensional and dynamic process based on the integration of competency-based, activity-oriented, project-based, interdisciplinary and STEM approaches. Its central objective is to develop a learner capable of transforming

knowledge into practical action, analysing technological problems, designing solutions, working creatively and critically, using appropriate technological and digital resources, and evaluating the social and environmental consequences of technological decisions.

Therefore, the theoretical foundations of technological competence formation should be built around the unity of knowledge, practical experience, technological thinking, creativity, problem-solving, digital literacy and responsible action. Such an approach corresponds to current transformations in European education and creates methodological prerequisites for updating technological education in Ukrainian secondary schools in accordance with contemporary competency-based and STEM-oriented educational priorities.

References

1. UNESCO International Bureau of Education. Competences: Curriculum on the Move. Thematic Note No. 19. Geneva : UNESCO International Bureau of Education, 2024. URL: <https://www.ibe.unesco.org/en/articles/competences> (дата звернення: 13.10.2026).

2. OECD. Promoting Students' Competencies and Effective Pedagogies for the 21st Century in the German-speaking Community of Belgium. OECD Education Policy Perspectives. 2024. No. 109. Paris : OECD Publishing. DOI: <https://doi.org/10.1787/fe5f6cfb-en> (дата звернення: 13.10.2026).

3. Pokropek A., Mazzeo Ortolani G., Karpinski Z., Biagi F. STEM Competencies, Challenges, and Measurements: A Literature Review. Luxembourg : Publications Office of the European Union, 2024. DOI: <https://doi.org/10.2760/9390011>. URL:

<https://publications.jrc.ec.europa.eu/repository/handle/JRC138618> (дата звернення: 13.10.2026).

4. European Commission. Promoting STEM Education in Schools. Luxembourg : Publications Office of the European Union, 2026. DOI: <https://doi.org/10.2766/9663751>. URL: <https://op.europa.eu/en/publication-detail/-/publication/cf2f8641-4a85-11f1-8095-01aa75ed71a1/language-en> (дата звернення: 13.10.2026).

5. OECD. PISA 2022 Results (Volume III): Creative Minds, Creative Schools. Paris : OECD Publishing, 2024. DOI: <https://doi.org/10.1787/765ee8c2-en> (дата звернення: 13.10.2026).

6. Vuorikari R., Kluzer S., Punie Y. DigComp 3.0: European Digital Competence Framework. 5th ed. Luxembourg : Publications Office of the European Union, 2025. DOI: <https://doi.org/10.2760/0001149> (дата звернення: 13.10.2026).

7. Giannoutsou N., Ioannou A., Timotheou S., Miliou O., Dimitriadis Y., Cachia R., Villagr -Sobrino S., Mart nez-Mon s A. Unpacking the Impact of Digital Technologies in Education: Literature Review and Assessment Framework. Luxembourg : Publications Office of the European Union, 2024. DOI: <https://doi.org/10.2760/214675>. URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC132998> (дата звернення: 13.10.2026).

Дата першого надходження рукопису до видання: 13.10.2026

Дата прийняття до друку рукопису після рецензування: 24.10.2026

Дата публікації: 27.10.2026

СЕКЦІЯ 15. ПСИХОЛОГІЧНІ НАУКИ**УДК: 316.6****ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ФОРМУВАННЯ СОЦІАЛЬНОЇ
ІДЕНТИЧНОСТІ ТА САМООЦІНКИ СУЧАСНОЇ МОЛОДІ**

Ничипорук Яна Олександрівна
здобувач вищої освіти факультету
публічного управління,
Хмельницький університет управління та
права імені Леоніда Юзькова
м. Хмельницький, Україна

Актуальність теми обумовлена наявністю того факту, що цифрова трансформація сучасного суспільства суттєво змінила традиційні інститути соціалізації, оскільки значна частина комунікативної та самопрезентаційної активності молоді перейшла у віртуальний простір. Соціальні мережі перестали бути просто засобом обміну повідомленнями та перетворилися на повноцінне середовище, де відбуваються складні внутрішньоособистісні та міжособистісні процеси. Постійна залученість до цифрового життя створює унікальний контекст для дорослішання, який має неоднозначний вплив на емоційне благополуччя, еволюцію самосприйняття та формування соціальної ідентичності підростаючого покоління.

Враховуючи актуальність теми, нами визначена *мета дослідження*: проаналізувати психологічні особливості впливу соціальних мереж на формування соціальної ідентичності та самооцінки сучасної молоді.

Вплив цифрових платформ відзначається вираженою дуалістичністю: як зазначають дослідники: «Соціальні мережі відіграють як позитивну, так і негативну роль у житті молоді: вони слугують простором для самовираження,

підтримки та розвитку соціальних зв'язків, водночас можуть стати джерелом психологічного навантаження, тривожності, емоційної нестабільності та формування залежної поведінки» [1, с. 100]. Виявлена суперечливість зумовлює актуальність глибокого аналізу того, як саме мережева активність і споживання цифрового контенту відображаються на формуванні соціальної ідентичності та самооцінних судженнях особистості.

Формування ідентичності в цифрову епоху перестало бути лінійним і передбачуваним процесом, оскільки віртуальне середовище надає молодій людині безпрецедентний ступінь свободи в конструюванні власного «Я». На відміну від реального життя, де соціальний статус, зовнішні дані та рольові очікування багато в чому обмежені фізичним та соціальним контекстом, у мережі молодь має змогу моделювати й експериментувати з різними варіаціями власного презентаційного образу, оскільки, як зазначає А. Краснякова: «Нове комунікативне інтернет-середовище – це "творча лабораторія по створенню ідентичностей", де особа має змогу "приміряти на себе ті чи інші ідентифікаційні симулякри", "гратися" з власною ідентичністю» [2, с. 3].

Прагнучи здобути схвалення однолітків, юнаки та дівчата часто вибудовують свій цифровий профіль не на основі реальних характеристик, а орієнтуючись на суб'єктивні уявлення про успішність та привабливість. Проте таке прагнення має й зворотню сторону, адже молоді люди створюють свою віртуальну ідентичність як проєкцію ідеального «Я», щоб справити враження. Цей метод може підвищити самооцінку як віртуально, так і в соціальній реальності. Також соціальна підтримка, отримана в соціальних мережах через онлайн-взаємодії сприяє формуванню ідентичності [3, с. 217].

Сприйняття власної особистості у віртуальному просторі значною мірою залежить від зовнішнього схвалення, яке в соціальних мережах матеріалізується

у вигляді позитивних відгуків, вподобайок та коментарів. Для молодшої людини цифрова аудиторія стає своєрідним дзеркалом, у якому вона шукає підтвердження власної значущості та цінності. Науковці підкреслюють, що відчуття затвердження та прийняття, які вони отримують, є важливими для розвитку здорової самооцінки й позитивного самовідчуття [4, с. 100]. Регулярна позитивна зворотна реакція допомагає молоді відчувати себе частиною спільноти та підвищує впевненість у власних силах.

Однак залежність від постійного схвалення та намагання підтримувати виключно бездоганний онлайн-образ неминуче призводять до викривлення самосприйняття. Коли між реальним життєвим досвідом особистості та її демонстраційним цифровим фасадом виникає глибока прірва, людина починає відчувати внутрішню розгубленість, втрачає чіткі орієнтири власної автентичності та стикається з емоційним виснаженням через необхідність відповідати створеному макету успішності.

Негативний вплив соціальних мереж суттєво посилюється через процес пасивного споглядання чужих профілів. Оскільки алгоритми цифрових майданчиків орієнтовані на популяризацію яскравого та відредагованого вмісту, користувачі отримують викривлене уявлення про чужий спосіб життя. Постійне зіставлення себе із цими ідеалізованими стандартами руйнує внутрішнє відчуття власної цінності. Як зазначають дослідники даної проблеми: «Соціальні мережі створюють можливість постійного порівняння себе з іншими людьми. Це викликає почуття незадоволення своїм життям, зовнішнім виглядом, досягненнями тощо. Як наслідок, молоді люди отримують психологічний стрес, низьку самооцінку та почуття неповноцінності» [5, с. 63]. Молодь починає сприймати природні складнощі чи власні недоліки як

особистісну неповноцінність, що провокує тривалу депресивність та розчарування в собі.

Масштаб цієї проблеми підтверджується численними емпіричними дослідженнями, які фіксують реальні зміни у психоемоційному стані молодих користувачів під впливом регулярного перегляду мережевого контенту. Постійний наплив ідеалізованої інформації створює надмірне сенсорне та емоційне навантаження, з яким незріла психіка не завжди здатна впоратися. Зокрема, у працях науковців вказується: «28 % респондентів зізналися у зниженні самооцінки після перегляду контенту в соціальних мережах, а 96 % відчують перевантаження через наплив інформації» [6]. Такі показники свідчать про те, що негативні наслідки занурення у віртуальний світ перестали бути поодинокими випадками і набули масового характеру.

Психологічний стан молоді також тісно пов'язаний із кількісними показниками використання гаджетів. Тривале безперервне перебування в мережі позбавляє людину можливості повноцінно відпочити, відновлювати емоційний ресурс та розвивати реальні навички комунікації. Дослідження показують, що зі збільшенням часу перебування у соціальних мережах знижується відвертість, цінність себе, прив'язаність до себе та підвищується внутрішньо особистісний конфлікт [7, с. 34]. Коли віртуальне спілкування повністю заміщує собою живі контакти, особистість втрачає здатність до глибокого емоційного обміну, стає більш замкненою та вразливою до стресів, а її самооцінка починає коливатися залежно від будь-якої зміни мережевої активності.

Окрім внутрішніх психологічних конфліктів та соціального порівняння, суттєвою загрозою для формування здорової самооцінки та соціальної ідентичності є деструктивні форми поведінки у віртуальному просторі, зокрема

кібербулінг, тролінг та агресивний онлайн-мобінг. Почуття анонімності й відсутність безпосереднього зорового контакту в мережі нерідко знижують поріг емпатії у користувачів, стимулюючи прояви віртуального тиску. Зі збільшенням часу, проведеного у соціальних мережах, для молодих людей суттєво зростають ризики стати жертвою агресивних дій, що провокує викривлення сприйняття власного іміджу та руйнує адекватні механізми самооцінювання. Систематичний негативний тиск у цифровому середовищі підриває базове відчуття безпеки молоді, викликає емоційну відстороненість від оточення та стає чинником глибокої психоемоційної кризи.

Усе це вказує на те, що для збереження ментального здоров'я молоді необхідний свідомий та збалансований підхід до споживання цифрового контенту. Потрібно навчатися критично сприймати інформацію в інтернеті, розуміти умовність та штучність багатьох віртуальних образів і не визначати власну цінність кількістю реакцій у соціальних мережах. Особливу роль у цьому процесі відіграє формування внутрішньої стійкості, адже наукові дані беззаперечно підкреслюють важливість розвитку емоційної стійкості та навичок критичного мислення серед молоді для подолання кризових явищ у цифровому середовищі.

Отже, соціальні мережі стали визначальним простором соціалізації сучасної молоді, який чинить глибокий і суперечливий вплив на формування її соціальної ідентичності та самооцінки. З однієї сторони, цифрові платформи розширюють можливості для комунікації та самопрезентації, а з іншої – створюють високі ризики для психоемоційного благополуччя. Постійне спостереження за ідеалізованим контентом, залежність від зовнішнього схвалення та загрози віртуальної агресії призводять до деформації усвідомлення власної особистості, зниження самоповаги та виникнення конфлікту між

реальним та бажаним образом себе. Подолання цих негативних наслідків вимагає розвитку цифрової грамотності та критичного ставлення молоді до мережевого контенту, а також системної соціально-психологічної підтримки у процесі формування її стійкої внутрішньої самооцінки.

Список використаних джерел

1. Шевчук О. В. Вплив соціальних мереж на психоемоційний стан молоді: соціальна робота з підлітками в еру цифрових технологій. Соціальна робота та психологія: освіта і наука. 2025. № 1. С. 98–101. DOI: <https://doi.org/10.32782/3041-1351/2025-1-17>. URL: <https://journals.kpdi.in.ua/index.php/swp/article/view/248>.
2. Краснякова А. О. Інтернет-середовище як новий комунікативний простір самопрезентації особистості. Наукові студії із соціальної та політичної психології. 2016. Вип. 38 (41). С. 286–297. URL: <https://lib.iitta.gov.ua/id/eprint/709506/1/HC%20№38%20-%202016-1.pdf>.
3. Рубан А. К. Вплив соціальних мереж на формування ідентичності підлітків та молоді. Науковий вісник Ізмаїльського державного гуманітарного університету. Серія: Педагогічні науки. 2021. Вип. 56. С. 213–220. URL: <https://visnyk.idgu.edu.ua/index.php/nv/article/view/507>.
4. Гудімова А. Х. Специфіка впливу соціальних мереж на психологічне благополуччя підлітків. Габітус. 2020. Вип. 12. Т. 2. С. 98–102. DOI: <https://doi.org/10.32843/2663-5208.2020.12-2.16>. URL: https://habitus.od.ua/journals/2020/12_2020/part_2/18.pdf.
5. Гречановська О. В., Мегем О. М., Потапюк Л. М. Вплив соціальних мереж на психологічний стан та самооцінку української молоді. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія:

Психологія. 2023. Т. 34 (73), № 4. С. 60–66. URL: https://psych.vernadskyjournals.in.ua/journal/4_2023/11.pdf.

6. Gołębiowska E. Oddziaływanie mediów społecznościowych na społeczne i emocjonalne funkcjonowanie młodych osób. Oświatologia. 2024. № 13. S. 50–58. DOI: <https://doi.org/10.28925/2412-124X.2024.13.5>. URL: <https://osvitologia.kubg.edu.ua/index.php/osvitologia/article/view/188/189>.

7. Березовська Л. І. Вплив соціальних мереж на психологічне благополуччя особистості. Вісник Національного університету оборони України. 2020. Вип. 2 (55). С. 28–36. DOI: <https://doi.org/10.33099/2617-6858-2020-55-2-28-36>. URL: <https://visnyk.nuou.org.ua/article/view/214059/214150>

Дата першого надходження рукопису до видання: 22.10.2026

Дата прийняття до друку рукопису після рецензування: 24.10.2026

Дата публікації: 27.10.2026

© Ничипорук Я.О., 2026

УДК: 316.6

ВПЛИВ ГРУПОВОГО ТИСКУ НА ПРИЙНЯТТЯ ОСОБИСТИХ РІШЕНЬ

Федоренко Віталіна Віталіївна,
здобувач вищої освіти факультету
публічного управління,
Хмельницький університет управління та
права імені Леоніда Юзькова
м. Хмельницький, Україна

Актуальність теми дослідження обумовлена наявністю того факту, що у сучасному суспільстві людина часто потрапляє в ситуації, в яких доводиться приймати рішення не лише на основі власних бажань і переконань, а й під впливом думки оточення. Особливо це помітно у великих колективах, де існують умовні певні правила, звичаї, традиції. І коли в колектив приходить нова людина у неї виникає бажання бути прийнятою, не виділятися серед інших та відповідати очікуванням. Через це людина іноді може погоджуватися з більшістю, навіть якщо її особиста думка відрізняється. Як наслідок виникає стан внутрішнього дисонансу, що негативно позначається на міжособистісних і між групових взаєминах.

Враховуючи актуальність теми, нами визначена мета дослідження: проаналізувати психологічні особливості впливу групового тиску на прийняття особистих рішень.

На прийняття рішень у житті людини впливають різні психологічні чинники. Насамперед це емоції, адже залежно від настрою людина може по-різному оцінювати ситуацію та робити певний вибір. Також важливе значення мають самопочуття, рівень стресу, втома та тривожність, оскільки

вони можуть заважати спокійно обдумати можливі варіанти. На рішення впливають і самооцінка, особисті переконання та життєві цінності, які визначають ставлення людини до різних обставин. Водночас важливу роль відіграє оточення, зокрема родина, друзі та однолітки. Їхні поради й думки можуть допомогти зробити правильний вибір, але іноді вони стають причиною того, що людина починає сумніватися у власній позиції та погоджується з більшістю. Особливо це проявляється тоді, коли людина боїться осуду або прагне отримати схвалення інших. У таких ситуаціях вона може приймати рішення не відповідно до власних бажань, а для того, щоб не відрізнятись від оточення. Крім цього, на вибір впливають життєвий досвід, отримані знання, індивідуальні особливості характеру та наявність необхідної інформації [1, С. 98-99].

На думку Волянчук Н. Ю., Ложкіна Г. В. та Фомича М. В. групові норми та правила відіграють важливу роль у регулюванні поведінки членів колективу й можуть впливати на їхні особисті рішення. У будь-якому колективі поступово формуються певні правила поведінки та норми, яких дотримується більшість його учасників. Через бажання бути частиною групи людина може приймати ці правила та підлаштовуватися під думку оточення, навіть якщо вона не повністю збігається з її власними переконаннями. Якщо ж хтось поводиться інакше або не погоджується з більшістю, він може зіткнутися з критикою, насмішками чи неприйняттям інших. У таких ситуаціях виникає тиск, який може змусити людину змінити свою поведінку або рішення, щоб не відчувати себе відокремленою від групи. Далі людина проявляється по-різному від групового тиску. Зокрема, конформіст – проявляється в тому, що людина погоджується з думкою більшості та змінює власну позицію під її впливом. Нонконформіст – характеризується прагненням відстоювати власні погляди й чинити опір тиску

оточення. Колективіст – людина яка погоджується з іншими лише тоді, коли вважає їхню позицію правильною та обґрунтованою [2, С.258].

Чорна Л. Г. розглядала, як складна життєва ситуація людини в колективі впливає на власну думку. Взаємодія людини з групою залежить не тільки від того, як вона сама сприймає певну ситуацію, а й від ставлення до неї інших учасників колективу. Люди можуть співчувати людині, яка пережила складні обставини, але водночас уникати спілкування з нею, оскільки не знають, як правильно поводитися в такій ситуації. Через це людина може поступово віддалятися від колективу та відчувати себе зайвою або неприйнятною. У групі також може виникати поділ на «своїх» і «чужих», що впливає на стосунки між її учасниками. Якщо складна ситуація відбувається безпосередньо в групі, реакція її членів може бути різною: від підтримки та згуртування до осуду й виключення людини з колективу. Це залежить від обставин, а також від правил і цінностей, прийнятих у групі [3, С.7]. Такий досвід може по-різному впливати на особистість: сприяти розвитку самостійності та стійкості або, навпаки, посилювати страх бути відкинутим і змушувати людину підлаштовуватися під думку більшості, тоді людина може відмовлятися від власних поглядів і діяти відповідно до очікувань оточення.

Важливе значення у прийнятті особистих рішень відіграє вплив авторитетних людей, думку яких людина вважає правильною та до якої прислухається. Це можуть бути батьки, вчителі, керівники або інші люди, які мають більше досвіду чи знань. У таких випадках людина часто довіряє їхнім порадам і може погоджуватися з ними, навіть не замислюючись над тим, чи відповідають вони її власним поглядам. Такий вплив може бути корисним, адже допомагає отримувати нові знання, уникати помилок і приймати обдумані рішення. Але варто враховувати, що надмірна довіра до авторитетної особи

може призвести до того, що людина перестає самотійно аналізувати ситуацію та покладається лише на чужу думку [4, С.17-18]. Це особливо важливо в контексті групового тиску, коли людина може погоджуватися з певним рішенням через повагу до лідера групи або страх піти проти його позиції. У результаті власні переконання можуть відійти на другий план, а рішення прийматимуться переважно під впливом інших.

Одним із проявів групового тиску є маніпуляція, за допомогою якої окремі люди або група намагаються вплинути на думки, почуття та поведінку людини у власних інтересах. При цьому людина може навіть не усвідомлювати, що на її рішення впливають інші, і вважати свій вибір самотійним. У колективі маніпуляція може проявлятися через викликання почуття провини, страху бути відкинутим або бажання отримати схвалення більшості. У таких ситуаціях людина може погоджуватися з думкою групи не тому, що справді її підтримує, а через небажання вступати в конфлікт або втрачати прихильність оточення. Такий вплив є особливо небезпечним, оскільки людина не завжди помічає, що її рішення продиктовані не власними переконаннями, а бажаннями інших [5, С.65].

Чутки є одним зі способів психологічного впливу, який може впливати на думки, поведінку та особисті рішення людини. Вони виникають і поширюються тоді, коли люди намагаються самотійно пояснити певні події або отримати інформацію, якої їм бракує. У групі чутки можуть формувати певне ставлення до людей чи ситуацій, впливати на думку більшості та спонукати людину погоджуватися з іншими. Якщо в колективі поширюється певна думка про людину або її вчинок, інші можуть почати її підтримувати, навіть не перевірявши достовірність інформації. Це може призводити до прийняття рішень під впливом оточення, а не власних переконань. Особливо небезпечними

є неправдиві чутки, оскільки вони можуть викликати страх, недовіру та сприяти поширенню хибних уявлень.

Навіювання (або сугестія) у ситуаціях групового тиску працює як спосіб психологічного впливу, коли людина приймає рішення й діє без глибокого логічного аналізу чи критичної оцінки того, що відбувається. У цей момент критичне мислення й самоконтроль просто вимикаються, тому інформація сприймається без жодних сумнівів. Такий вплив передається через чіткі слова, жести чи навіть вираз обличчя. Вони не змушують думати й аналізувати, а одразу підштовхують зробити так, як вимагають. Часто буває, що коли один учасник групи першим виконує команду чи підкоряється, усі інші починають просто повторювати за ним [6, С.63-34].

Під впливом групового тиску людина може по-різному реагувати на думку більшості, тому виділяють два основні види конформної поведінки: зовнішнє та внутрішнє підпорядкування. Зовнішнє підпорядкування проявляється тоді, коли людина погоджується з думкою більшості та поводить себе відповідно до неї, хоча насправді може мати іншу позицію. У такому випадку вона може діяти так через страх осуду, бажання уникнути конфлікту або прагнення бути прийнятою в колективі. Внутрішнє підпорядкування, навпаки, виникає тоді, коли людина не просто погоджується з групою зовні, а й сама починає поділяти її погляди та сприймати їх як власні. Така зміна думки може зберігатися навіть тоді, коли людина вже не перебуває під безпосереднім впливом групи [7, С.486].

Отже, груповий тиск є одним із чинників, що впливає на прийняття особистих рішень та поведінку людини. На вибір особистості можуть впливати групові норми, думка більшості, авторитет інших людей, маніпуляції, чутки та навіювання. Під дією цих чинників людина може змінювати власну позицію,

пристосовуватися до очікувань оточення або відмовлятися від своїх переконань. Реакція на груповий тиск залежить від індивідуальних особливостей особистості, її самооцінки, життєвого досвіду та здатності критично оцінювати інформацію. Зокрема, конформна поведінка може проявлятися як зовнішнє погодження з думкою групи без зміни власних переконань або як внутрішнє прийняття групової позиції. Таким чином, вплив групового тиску на прийняття особистих рішень має різні прояви та визначається як особливостями соціального середовища, так і психологічними характеристиками самої людини.

Список використаних джерел

1. Пріснякова Л. М., Агапова І. М. Вплив психологічних чинників на процес прийняття життєвих рішень особистістю. Technologies and Strategies for the Implementation of Scientific Achievements : збірник наукових праць VIII Міжнародної науково-теоретичної конференції (м. Стокгольм, Швеція, 5 вересня 2025 р.). Collection of Scientific Papers «SCIENTIA». 2025. С. 95–103. URL: <https://previous.scientia.report/index.php/archive/article/view/2885/2915>.
2. Волянчук Н. Ю., Ложкін Г. В., Фомич М. В. Командна згуртованість як соціально-психологічний феномен. Габітус. 2022. Вип. 36. С. 255–259. DOI: <https://doi.org/10.32843/2663-5208.2022.36.42>. URL: <https://habitus.od.ua/journals/2022/36-2022/42.pdf>.
3. Проблемна взаємодія в групах: феноменологія, чинники, профілактика : монографія / Л. Г. Чорна, П. П. Горностай, О. В. Яремчук, В. І. Вус, О. Л. Коробанова, О. Т. Плетка ; за наук. ред. Л. Г. Чорної ; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Кропивницький : ІМЕКС-ЛТД, 2021. 112 с. URL:

<https://lib.iitta.gov.ua/id/eprint/729979/1/ПРОБЛЕМНА-ВЗАЄМОДІЯ-В-ГРУПАХ-.pdf>.

4. Коломейчук І. П. Порівняльний аналіз форм психічної активності та стратегій психологічного впливу особистості : кваліфікаційна робота магістра за спеціальністю 053 «Психологія» / Західноукраїнський національний університет. Тернопіль, 2025. 84 с. URL: <https://api.dspace.wunu.edu.ua/api/core/bitstreams/02a457a0-c952-45cc-a64d-7e6f34a8024d/content>.
5. Сурякова М. В., Панфілова Г. Б., Склянська О. В. Соціальна психологія (з основами соціально-психологічного тренінгу) : навч. посіб. Дніпро : Середняк Т. К., 2021. 150 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059460.pdf>.
6. Гуменюк О. Концепції психологічного впливу в сучасній психології. Психологія і суспільство. 2003. № 1 (11). С. 34–89. URL: <https://pis.wunu.edu.ua/index.php/uapis/article/view/93>.
7. Шевченко О. М. Психологічні особливості конформізму в групі здобувачів вищої освіти. Соціально-освітні домінанти професійної підготовки сучасного компетентнісного фахівця : збірник матеріалів IV Всеукраїнської студентської науково-практичної конференції. Біла Церква, 2025. С. 485–488. URL: <https://binpo.com.ua/wp-content/uploads/2025/06/Збірник-матеріалів-студентської-конференції2.pdf#page=485>

Дата першого надходження рукопису до видання: 21.10.2026

Дата прийняття до друку рукопису після рецензування: 24.10.2026

Дата публікації: 27.10.2026

СЕКЦІЯ 16. МЕДИЧНІ НАУКИ

УДК 616.36-053.2:575.1

КОМПЛЕКСНА ДІАГНОСТИКА СПАДКОВОГО ХОЛЕСТАЗУ У ДІТЕЙ

Бевзюк Анастасія Євгеніївна,
здобувачка вищої освіти медичного факультету,
Ужгородський університет

Науковий керівник:
Шейко Лариса Павлівна
к.ю.н, доцент кафедри медичної та лабораторної генетики
Національний університет охорони здоров'я України
імені П.Л. Шупика

Молекулярна діагностика спадкового холестазу в дітей потребує узгодження результатів секвенування з клінічними та біохімічними даними. Подібна картина жовтяниці й порушення функції печінки може супроводжувати захворювання з різними механізмами успадкування та позапечінковими проявами. Міжнародні рекомендації визначають холестатичну жовтяницю немовлят як патологічний стан, що потребує своєчасної діагностики [1]. Поєднання клінічних і біохімічних даних з молекулярно-генетичним тестуванням допомагає визначити причину захворювання та обґрунтувати подальше обстеження.

Метою роботи є оцінка діагностичної результативності молекулярно-генетичного тестування при спадковому холестазі в дітей та визначення значення клінічного відбору й інтерпретації генетичних варіантів.

Здійснено огляд, порівняльний аналіз та узагальнення наукових публікацій, індексованих у базі даних PubMed, щодо діагностичної

результативності молекулярно-генетичного тестування при спадковому холестази у дітей. Проаналізовано п'ять досліджень та міжнародні рекомендації з діагностики холестазу й інтерпретації генетичних варіантів.

За результатами дослідження виявлено, що молекулярно-генетичне тестування дозволяє встановити спадкову причину холестазу в частини дітей, а його діагностична результативність залежить від клінічного відбору пацієнтів та складу досліджуваної вибірки. У проспективній когорті зі 125 дітей із неонатальним та інфантильним холестазом генетичне обстеження виконано 50 відібраним пацієнтам. Застосування аналізу одного гена, генних панелей або секвенування екзому у форматі тріо дозволило виявити генетичну причину захворювання у 60 % цієї обстеженої підгрупи [2].

Результати панельного секвенування також відрізнялися залежно від досліджуваної групи. Використання панелі з 34 генів у 602 дітей із холестазом забезпечило встановлення підтвердженого молекулярного діагнозу у 169 пацієнтів (28,1 %) [3]. У меншій клінічно відібраній групі, що включала, зокрема, дітей із фенотипом прогресуючого сімейного внутрішньопечінкового холестазу з низькою активністю гамма-глутамілтрансферази, молекулярне підтвердження отримано у 15 із 22 пацієнтів (приблизно 68 %) [4].

У масштабніших програмах тестування встановлено нижчі частки позитивних діагностичних результатів. Аналіз панелі з 66 генів у 2171 пацієнта продемонстрував загальну діагностичну результативність 12 %, що відповідало 265 позитивним результатам. Водночас було виявлено 3117 варіантів невизначеного значення [5]. У вибірці з 10 894 зразків дітей і дорослих частка підтверджених молекулярних діагнозів становила 6,8 %, а частка потенційних діагнозів дорівнювала 2,2 %. Пацієнтам віком до одного року належали 51,1 % зразків, тому ці показники характеризують змішану вікову вибірку [6].

Зіставлення наведених результатів вказує на необхідність урахування клінічних характеристик пацієнтів, критеріїв їхнього відбору та визначення позитивного результату. Висока результативність у відібраних групах сама по собі не доводить переваги конкретної генної панелі. Підтверджені та потенційні молекулярні діагнози необхідно аналізувати окремо. Інтерпретація генетичних знахідок передбачає розмежування патогенних, імовірно патогенних, невизначеного значення, імовірно доброякісних і доброякісних варіантів.

Висновки. Молекулярно-генетичне тестування є важливою складовою комплексної діагностики спадкового холестази в дітей. Його результативність залежить від клінічних характеристик пацієнтів, критеріїв відбору та інтерпретації генетичних варіантів. Поєднання клінічних, біохімічних і генетичних даних дозволяє обґрунтовувати молекулярний діагноз та визначати потребу в подальшому обстеженні.

Список використаних джерел

1. Fawaz R., Baumann U., Ekong U. et al. Guideline for the Evaluation of Cholestatic Jaundice in Infants. *Journal of Pediatric Gastroenterology and Nutrition*. 2017. Vol. 64, No. 1. P. 154-168. DOI: 10.1097/MPG.0000000000001334.
2. Nicastro E., Di Giorgio A., Marchetti D. et al. Diagnostic Yield of an Algorithm for Neonatal and Infantile Cholestasis Integrating Next-Generation Sequencing. *The Journal of Pediatrics*. 2019. Vol. 211. P. 54-62.e4. DOI: 10.1016/j.jpeds.2019.04.016.
3. Almes M., Spraul A., Ruiz M. et al. Targeted-Capture Next-Generation Sequencing in Diagnosis Approach of Pediatric Cholestasis. *Diagnostics*. 2022. Vol. 12, No. 5. Article 1169. DOI: 10.3390/diagnostics12051169.

4. Lipiński P., Ciara E., Jurkiewicz D. et al. Targeted Next-Generation Sequencing in Diagnostic Approach to Monogenic Cholestatic Liver Disorders-Single-Center Experience. *Frontiers in Pediatrics*. 2020. Vol. 8. Article 414. DOI: 10.3389/fped.2020.00414.
5. Karpen S. J., Kamath B. M., Alexander J. J. et al. Use of a Comprehensive 66-Gene Cholestasis Sequencing Panel in 2171 Cholestatic Infants, Children, and Young Adults. *Journal of Pediatric Gastroenterology and Nutrition*. 2021. Vol. 72, No. 5. P. 654-660. DOI: 10.1097/MPG.0000000000003094.
6. Hoskins B. J., Pramparo T., Gough E. et al. Clinical utility of an evolving cholestasis gene panel in 10,000 children and adults. *Frontiers in Pediatrics*. 2026. Vol. 14. Article 1841006. DOI: 10.3389/fped.2026.1841006.

Дата першого надходження рукопису до видання: 06.10.2026

Дата прийняття до друку рукопису після рецензування: 11.10.2026

Дата публікації: 27.10.2026

**New horizons of science:
interdisciplinary research in a changing world**

international scientific and practical conference

27.10.2026 – Uzhhorod, Ukraine – Prague, Czech Republic
collection of scientific papers