

УДК 342.951.2(477)

Олег ШИМІН

Національний університет “Львівська політехніка”,
аспірант Навчально-наукового інституту права,
психології та інноваційної освіти
oleh.p.shymin@lpnu.ua
ORCID: 0009-0008-3134-0178

ВИКЛИКИ ДЛЯ ЕЛЕКТРОННОГО ПРАВОСУДДЯ

<http://doi.org/10.23939/law2025.47.333>

© Шимін О., 2025

У статті проведено комплексний аналіз викликів для електронного правосуддя у сучасному глобалізованому суспільстві. Для досягнення мети потрібне використання авторської методології, що репрезентує систему методів та підходів, які дають змогу дійти обґрунтованих висновків, основним серед яких є синергетичний підхід.

Використовуючи звіти міжнародних органів та інституцій, європейські статистичні дані, праксіологічний аналіз практики застосування електронного правосуддя в Україні та компаративне дослідження визначеної проблематики в окремих державах ЄС дало можливість узагальнити виклики для електронного правосуддя у наступні три групи: технічного, безпекового та інтелектуального характеру. До першої групи належать проблеми, що пов’язані з застарілим комп’ютерним забезпеченням, мережа та сервери часто можуть не відповідати новітнім процесам та технологіям, брак доступу до мережі “Інтернет”, проблеми з електропостачанням, незабезпеченість належним обладнанням чи технічною підтримкою суддів для вільного користування новітніми можливостями та технологіями. Тому доволі проблемно відновлювати судочинство в умовах загроз життю населення під час війни. Зазначимо, що загалом судова система досить ефективно долає труднощі такого характеру. Технічні труднощі існують у цифровому суспільстві завжди, але в умовах війни, фінансово-економічних проблем держави такі загрози особливо актуалізуються.

Проблеми безпекового характеру містять загрози внутрішніх та зовнішніх кібератак, що впливає як на функціонування суду, так і на доброчесність її представників. Прокритиковано вимоги щодо вимкнення блокувальників реклами, VPN-сервісів, проксісерверів та антивірусних програми, які містяться в Інструкції користувача підсистеми відеоконференцз’язку ЄСІТС: затверджена Наказом ДП “Інформаційні судові системи” від 22.10 2024 року. Мотивовано, що за таких умов комп’ютерні системи суду залишаються відкритими для кіберзагроз, вказане створює потенційні ризики для атак, оскільки відкриті канали відеоконференції залишаються незахищеними, можливе перехоплення трафіку під час сервісного з’єднання. Також умотивовано, що така норма створює перепони доступу до суду великій кількості громадян, що перебувають тимчасово за кордоном у зв’язку з військовими загрозами.

Належна технологічна освіта учасників процесу, представників адвокатури та суддівського корпусу, працівників суду – це ще один виклик інтелектуального характеру, з яким стикається електронне правосуддя в сучасних умовах розвитку цифрової реальності.

Ключові слова: електронне правосуддя, цифровізація, діджиталізація, доступ до суду, глобалізація, загрози, судочинство, кібератаки, національна безпека, судова система, війна, правове регулювання.

Постановка проблеми. Діджиталізація дуже стрімко, активно та, найвірогідніше, безповоротно ввійшла в життя людей, судова система у сфері цифровізації не є винятком. Проте треба звернути увагу, що все таки ця сфера повільніше ніж сфера приватного бізнесу та державного управління трансформує свою діяльність відповідно до оновлених можливостей.

Наукова думка та юридична практика здебільшого позитивно охарактеризує електронне судочинство, описуючи його як позитивний метод правосуддя, що застосовує дистанційні та віртуальні засоби, котрі допомагають скоротити витрати учасників судового процесу як матеріального, так і часового характеру, убезпечують від корупційних проявів, доступність та відкритість правосуддя, ефективність суддів, оптимізація судового навантаження тощо.

Проте, на нашу думку, абсолютизувати електронне правосуддя лише як явище новітньої реальності, що зумовлює тільки позитивні чинники, не потрібно, оскільки в процесі впровадження нового способу комунікації між суб'єктами судового процесу виникають також загрози, що спричиняють не тільки технічні труднощі, але й можуть стати загрозою для реалізації права на справедливий суд у державі.

Тому цінним для загальнотеоретичної юриспруденції та правової практики є визначення деструктивних чинників, які можуть супроводжувати електронне судочинство як новітній, інноваційний метод ведення правосуддя. Вказаному й присвячена ця наукова праця.

Аналіз дослідження проблеми. Проблематику вдосконалення правосуддя, реформування судової системи в аспекті її відповідності європейським стандартам порушували такі науковці, як Н. Ортинська, В. Ковальчук. Проблеми глобалізації суспільства та функціонування органів влади в умовах віртуалізації суспільства розглядала в своїх працях І. Жаровська. В. Берч, Ю. Бисага порушували питання конституційного регулювання електронного правосуддя в Україні.

Проте, враховуючи брак комплексного дослідження проблематики та невизначену синергетичну форму функціонування досліджуваного предмета, потрібний аналіз проблематики в контексті деструктивних викликів суспільної та правової реальності сьогодення на електронне правосуддя у демократичній державі.

Метою статті є комплексний аналіз викликів для електронного правосуддя у сучасному глобалізованому суспільстві. Для досягнення мети потрібне використання авторської методології, що репрезентує систему методів та підходів, котрі дають змогу дійти обґрунтованих висновків. Серед них вагомим є синергетичний підхід, оскільки неможливо передбачити розвиток електронного правосуддя в наступні етапи генезису, оскільки біфуркаційна точка, в якій зараз перебуває досліджуване правове явище, зумовлює різносторонність векторів впливу та її рух залежить від важкопередбачуваних технічних, технологічних, організаційних, політичних, інформаційних, соціальних процесів.

Виклад основного матеріалу. Інформаційні технології активно підтримують судочинство, судові процедури та діловодство у судах, зокрема інтегровані платформи правосуддя. Пандемічна загроза активізувала процес віртуалізації публічної влади, створила загальну практику реалізації та

захисту прав й законних інтересів громадян та юридичних осіб. Узагальнюючи, саме криза продемонструвала ті можливі переваги, що надає електронне правосуддя.

Унікальним є досвід України в цьому контексті, оскільки, перебуваючи у стані війни з державою-агресором, електронне правосуддя стало тим чинником, що дав змогу встояти державі, державному апарату в умовах військових дій та воєнних загроз для цивільного населення. Брак дієвого механізму захисту девальвує всю систему правосуддя в державі, породжує анархію, загрожує порушенням справедливості та верховенства права. Цифровізація судової діяльності поряд з іншими чинниками допомогла на первинних етапах повномасштабного вторгнення й надалі підтримує здійснення судочинства відповідно до загальновизнаних міжнародних та європейських стандартів.

Провідні експерти відзначають, що електронне правосуддя натомість не є легким процесом. Існують специфічні проблеми або ризики, пов'язані з цифровізацією цієї сфери, такі як делікатність процесів, правові обмеження, забезпечення незалежності судової влади, проектування системи, хороший користувацький досвід та висока сумісність. Вони відзначають, що через порівняно незрілий характер та різноманітність систем електронного правосуддя, що використовуються у всьому світі, все ще бракує інтегрованої дослідницької бази, яка б окреслювала конкретні сфери та теми досліджень електронного правосуддя та визначала майбутні напрями досліджень [1]. Треба визнати, що, як будь-яке новітнє явище, електронне правосуддя перехідного етапу породжує низку проблем, про які треба говорити предметніше.

Звіти міжнародних органів та інституцій, європейські статистичні дані, праксіологічний аналіз практики застосування електронного правосуддя в Україні та компаративне дослідження визначеної проблематики в окремих державах ЄС дало нам можливість узагальнити виклики для електронного правосуддя у наступні три групи: технічного, безпекового та інтелектуального характеру.

Розглянемо їх детальніше.

Виклики технічного характеру. Для функціонування електронного правосуддя повинна діяти спеціально розроблена для цього система. В Україні це Єдина судова інформаційно-телекомунікаційна система (ЄСІТС), що діє на підставі Закону України № 1416-IX “Про внесення змін до деяких законодавчих актів щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи” [2]. Цей нормативно-правовий акт узгоджує особливості функціонування електронного правосуддя з принципами та положеннями галузевого процесуального законодавства.

Безпосереднє функціонування системи ЄСІТС в судах та окремих модулів системи регулюється технічно Положенням про порядок функціонування окремих підсистем (модулів) судової інформаційної системи [3], що затверджено рішенням Вищої Ради правосуддя 17 серпня 2021 року. Проте той факт, що протягом часу функціонування до Положення вже чотири рази вносилися суттєві зміни (січень, лютий 2022 року, жовтень 2023, березень 2024 року), які технологічно оновлюють та трансформують систему, вказує на пошук оптимальних технічних та технологічних можливостей для належної та ефективної роботи електронного правосуддя в умовах військових викликів та загроз.

Серед технологічних проблем визначається те, що в судовій системі існують технічні проблеми, що пов'язані зі застарілим комп'ютерним забезпеченням, мережа та сервери часто можуть не відповідати новітнім процесам та технологіям, брак доступу до мережі “Інтернет”, проблеми з електропостачанням, незабезпеченість належним обладнанням чи технічною підтримкою суддів для вільного користування новітніми можливостями та технологіями.

За інформаційними даними, що надав Верховний Суд України, за станом на 2024 рік, знищено чи пошкоджено 131 будівлю суду (15 з них – вщент знищені, 116 – пошкоджені) [4]. Тому доволі проблемно відновлювати судочинство в умовах загроз життю населення під час війни. Зазначимо, що загалом судова система досить ефективно долає труднощі такого характеру. Технічні труднощі існують у цифровому суспільстві завжди, але в умовах війни, фінансово-економічних проблем держави такі загрози особливо актуалізуються.

Також, за даними авторського опитування суддів та працівників суду, що проводилися нами у Львівській області протягом 2023–2025 року (загальна кількість респондентів – 112 осіб), 74 %

вказали на те, що часто в своїй роботі під час використання ЄСІДС існують технічні збоїв, зависання програм, а також зависання сервісів. Також 65 % повідомили про те, що вони мають інформацію про існування складностей під час користування системою електронного документообігу, котрі полягають в різному форматуванні файлів, завантаженні документів, несистематизованості їх у процесі пошуку, значною кількістю спаму, труднощах із підписом документів тощо.

Виклики безпекового характеру. Серед останніх масових кібератак відзначаємо особливо негативний вплив їх на роботу всієї правової та державної системи України атаки, що відбулася 19 грудня 2024 року. Зовнішня кібератака спрямовувалася на державні реєстри України, але зачепила функціонування Електронного кабінету Електронного суду, зокрема протягом місяця (роботу було відновлено 20 січня 2025 року) були недоступними такі дії, як реєстрація електронного кабінету для юридичних осіб, для нових керівників юридичних осіб такий кабінет також був недоступним, перегляд текстів документів виконавчого провадження, отримання певних довідок з державних реєстрів.

Також знаходимо інформацію про те, що судові інституції, їхні електронні адреси можуть використовуватися зловмисниками з метою поширення неправомірної інформації, що загрожує нормальному функціонуванню суду, його апарату. Зокрема, у вересні 2024 року судова влада повідомила про здійснення хакерської розсилки повідомлень нібито з електронної адреси Західного апеляційного господарського суду [5].

Вказане демонструє нестійкість електронного судочинства до кібератак, а також взаємопереплетеність цифровізації держави, що свідчить про потребу пошуку додаткових, альтернативних технічних можливостей та їх унормування в національному законодавстві у разі кризових інформаційних загроз, які можуть відбуватися в майбутньому.

В контексті військових інформаційних загроз позитивно оцінюємо те, що Міністерство оборони України створило спеціальну структуру, яка фахово працює над відбиттям хакерських атак на органи публічної влади України – Центру реагування на кіберінциденти.

Кібератаки – це не тільки засоби ведення сучасної війни, але й загроза національній безпеці держави в мирний час. Зокрема, за даними США у липні 2024 року Вищий суд округу Лос-Анджелес став жертвою атаки програми-вимагача. Цей інцидент змусив закрити всі 36 будівель суду наступного понеділка для усунення порушення, яке вплинуло на системи управління справами суду, зокрема портал My Jury Duty та його головний вебсайт [6].

Проблема вимагачів у мережі “Інтернет” має особливо загрозливий характер. В штаті Джорджія в січні 2024 року відбувалася глобальна атака, за яку відповідальність взяла група вимагачів LockBit. Вона спричинила зупинку більшої частини державних послуг, від видачі реєстраційних документів на транспортні засоби та свідоцтв про шлюб до можливості суду обробляти юридичні документи онлайн. Хакери погрожували розкрити конфіденційні дані, зокрема потенційно гучну інформацію, пов’язану з поточними кримінальними справами. Місцева влада відмовилася від плати вимагачам, тому судова система не працювала понад місяць [7].

Ще один інформаційно-правовий аспект, який свідчить про потребу доопрацювання правового регулювання електронного правосуддя в Україні.

Інструкція користувача підсистеми відеоконференцзв’язку ЄСІТС: затверджена Наказом ДП “Інформаційні судові системи” від 22.10 2024 року містить вагоме застереження: “Не залежно від браузера, ОС та пристрою, блокувальники реклами, VPN-сервіси, проксі сервери та антивірусні програми можуть перешкоджати нормальній роботі сервісу, тому їх необхідно обов’язково відключити або налаштувати належним чином до початку конференції” [8]. Вказане свідчить, що під час такої дії комп’ютерні системи суду залишаються незахищеними, вказане створює потенційні ризики для атак, оскільки відкриті канали відеоконференції залишаються незахищеними. Також додамо, що технічний персонал щоразу змушений вимикати та вмикати захисті елементи, що значно ускладнює роботу та може спричинити ситуацію, за якої не тільки на строк відеоконференції, а загалом протягом

роботи суду він залишатиметься без захисту навіть від типових кібератак. Також можливе перехоплення трафіку під час сервісного з'єднання.

За час військових дій після повномасштабного вторгнення територію нашої держави покинули мільйони громадян, котрі нині перебувають в інших державах. Такі громадяни та й іноземці для безпечного доступу до національних ресурсів, у тому числі реалізації права доступу до суду використовують VPN для безпечного доступу до українських ресурсів. ЄСІТС містить значну кількість приватної інформації, зокрема не тільки персональні дані, але й документи приватного характеру, використовуючи технологію VPN вони убезпечують себе в сфері цифрової приватності. Тому в контексті забезпечення цифрової стійкості національної системи правосуддя доречно створити можливість доступу учасникам судового процесу через VPN-сервіси.

Виклики інтелектуального характеру. Розвиток технологій потребує належного рівня знань та технічних навиків учасників процесу. Нині вже не йдеться про користування комп'ютерною технікою, гаджетами, а потрібні знання суддів та працівників суду, особливо секретарів, під час роботи в системі “Електронний суд” та в режимі відеоконференцій. Загалом вказане породжує як когнітивні, так і організаційно-освітні виклики.

Без належної технічної освіти учасникам процесу важко орієнтуватися в процесах, технологіях та засобах, які щоразу розвиваються і стрімко прогресують. На державному рівні потрібно зробити акцент на цілеспрямованому навчанні суддів, секретарів судового засідання, адвокатів та інших зацікавлених осіб щодо роботи системи електронного правосуддя.

Висновки. Швидкість, ефективність, низький рівень енергетичних та фінансових витрат, зручність, перехід на позапаперову систему діловодства тощо вважається суттєвими досягненнями електронного судочинства у цифровій державі. Електронне правосуддя в умовах пандемічної загрози та військових дій є належним засобом реалізації права людини на доступ до суду.

Проте сучасні умови розвитку системи електронного судочинства визначають виклики технічного, безпекового та інтелектуального характеру, що впливають на нормальне його функціонування в умовах, яких перебуває нині українська держава. До першої групи належать проблеми, що пов'язані із застарілим комп'ютерним забезпеченням, мережа та сервери часто можуть не відповідати новітнім процесам та технологіям, брак доступу до мережі “Інтернет”, проблеми з електропостачанням, незабезпеченість належним обладнанням чи технічною підтримкою суддів для вільного користування новітніми можливостями та технологіями. Проблеми безпекового характеру містять загрози внутрішніх та зовнішніх кібератак, що впливає як на функціонування суду, так і на доброчесність її представників. Належна технологічна освіта учасників процесу, представників адвокатури та суддівського корпусу, працівників суду – це ще один виклик інтелектуального характеру, з яким стикається електронне правосуддя в сучасних умовах розвитку цифрової реальності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yavuz N., Karkin N., Yildi, M. *E-Justice: A Review and Agenda for Future Research*. In: Charalabidis, Y., Flak, L.S., Viale Pereira, G. (eds) *Scientific Foundations of Digital Governance and Transformation*. Public Administration and Information Technology, 2022. Vol. 38. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-92945-9_15 (Accessed: 20.04.2025).
2. Про внесення змін до деяких законодавчих актів щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи: Закон України від 29.06.2023 № 3200-IX. *База даних “Законодавство України” / ВР України*. 2023, № 81, ст. 297.
3. Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи: рішення БПІ від 17 серпня 2021 року № 1845/0/15-21. URL: https://hcj.gov.ua/sites/default/files/field/file/polozhennya_yesits_7.03.2024.pdf (Дата звернення: 20.04.2025).
4. Судочинство під час війни: судді ВС розповіли про виклики та особливості здійснення правосуддя в умовах воєнного стану. URL: <https://court.gov.ua/archive/1576192/> (Дата звернення: 20.04.2025).

5. Західний Господарський апеляційний суд. До уваги учасників судового процесу та користувачів судових послуг! URL: <https://wag.court.gov.ua/sud4870/pres-centr/general/1667916/> (Дата звернення: 20.04.2025).
6. LA County's Response to Impacts of LA County Superior Court Closure. URL: <https://lacounty.gov/court/> (Accessed: 20.04.2025).
7. Martinez A. Cyberattacks On U.S. Courts: Vulnerabilities, Impacts, And Response Strategies. URL: <https://www.forbes.com/sites/alonzomartinez/2024/08/30/cyberattacks-on-us-courts-vulnerabilities-impacts-and-response-strategies/> (Accessed: 20.04.2025).
8. Інструкція користувача підсистеми відеоконференцзв'язку ЄСІТС: затверджена Наказом ДП "Інформаційні судові системи" від 22. 10. 2024 року. URL: <https://surli.cc/tbdxbd> (Дата звернення: 20.04.2025).

REFERENCES

1. Yavuz, N., Karkin, N., Yildi, M. (2022). *E-Justice: A Review and Agenda for Future Research*. In: Charalabidis, Y., Flak, L. S., Viale Pereira, G. (eds.). Scientific Foundations of Digital Governance and Transformation. Public Administration and Information Technology, 38. Springer, Cham. Retrieved from: https://doi.org/10.1007/978-3-030-92945-9_15 (Accessed: 20.04.2025). [In English].
2. *Pro vnesennia zmin do deiakykh zakonodavchykh aktiv shchodo zabezpechennia poetapnoho vprovadzhennia Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy* [On Amendments to Certain Legislative Acts to Ensure the Phased Implementation of the Unified Judicial Information and Telecommunication System]: Zakon Ukrainy No. 3200-IX vid 29.06.2023. Baza danykh "Zakonodavstvo Ukrainy" / VR Ukrainy. 81, 297 [In Ukrainian].
3. *Polozhennia pro poriadok funktsionuvannia okremykh pidsystem (moduliv) Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy* [Regulations on the Procedure for the Functioning of Certain Subsystems (Modules) of the Unified Judicial Information and Telecommunication System]: rishennia VRP vid 17 serpnia 2021 roku No. 1845/0/15-21. Baza danykh "Zakonodavstvo Ukrainy" / VR Ukrainy. Retrieved from: https://hcj.gov.ua/sites/default/files/field/file/polozhennya_ysesits_7.03.2024.pdf (Accessed: 20.04.2025). [In Ukrainian].
4. *Sudochynstvo pid chas viiny: suddi VS rozpovily pro vyklyky ta osoblyvosti zdiisnennia pravosuddia v umovakh voiennoho stanu* [Judicial proceedings in time of war: judges of the Supreme Court spoke about the challenges and peculiarities of administering justice under martial law]. (2024). Retrieved from: <https://court.gov.ua/archive/1576192/> (Accessed: 20.04.2025). [In Ukrainian].
5. *Zakhidnyi Hospodarskyi apeliatsiinyi sud* [Western Commercial Court of Appeal]. (2024). Do uvahy uchasnykiv sudovoho protsesu ta korystuvachiv sudovykh posluh! Retrieved from: <https://wag.court.gov.ua/sud4870/pres-centr/general/1667916/> (Accessed: 20.04.2025). [In Ukrainian].
6. *LA Countys Response to Impacts of LA County Superior Court Closure*. (2024). Retrieved from: <https://lacounty.gov/court/> (Accessed: 20.04.2025). [In English].
7. Martinez, A. (2024). *Cyberattacks On U. S. Courts: Vulnerabilities, Impacts, And Response Strategies*. Retrieved from: <https://www.forbes.com/sites/alonzomartinez/2024/08/30/cyberattacks-on-us-courts-vulnerabilities-impacts-and-response-strategies/> (Accessed: 20.04.2025). [In English].
8. *Instruktsiia korystuvacha pidsystemy videokonferentsv'язku YeSITS* [User's manual of the videoconferencing subsystem of the EUIITS]: (2024). Zatverdzhena Nakazom DP "Informatsiini sudovi systemy" vid 22. 10. 2024 roku. Retrieved from: <https://surli.cc/tbdxbd> (Accessed: 20.04.2025). [In Ukrainian].

Дата надходження статті: 03.05.2025 р.

Oleg SHYMIN

Lviv Polytechnic National University,
Educational and Research Institute of Law,
Psychology and Innovative Education,
Postgraduate student
oleh.p.shymin@lpnu.ua
ORCID: 0009-0008-3134-0178

CHALLENGES FOR ELECTRONIC JUSTICE

The article provides a comprehensive analysis of the challenges for electronic justice in a modern globalized society. To achieve the goal, it is necessary to use the author's methodology, which represents a system of methods and approaches that will allow reaching substantiated conclusions, the main one of which is the synergistic approach.

Using reports of international bodies and institutions, European statistical data, praxeological analysis of the practice of applying electronic justice in Ukraine and a comparative study of certain issues in individual states, the EU has provided an opportunity to summarize the challenges for electronic justice into the following three groups: technical, security and intellectual. The first group includes problems related to outdated computer software, the network and servers may often not meet the latest processes and technologies, lack of access to the Internet, problems with power supply, lack of proper equipment or technical support for judges to freely use the latest capabilities and technologies. Therefore, it is quite problematic to restore judicial proceedings in conditions of threats to the lives of the population during the war. By the way, I would like to note that in general the judicial system overcomes difficulties of this nature quite effectively. Technical difficulties always exist in a digital society, but in conditions of war, financial and economic problems of the state, such threats are especially relevant.

Security problems include threats of internal and external cyberattacks, which affects both the functioning of the court and the integrity of its representatives. The requirements for disabling ad blockers, VPN services, proxy servers and antivirus programs contained in the User Manual of the EUIITS video conferencing subsystem: approved by the Order of the State Enterprise "Information Court Systems" dated 22.10.2024 are criticized. It is motivated that under such conditions, the court's computer systems remain open to cyber threats, which creates potential risks for attacks, since open video conferencing channels remain unprotected, and traffic may be intercepted during the service connection. It is also motivated that such a norm creates obstacles to access to the court for a large number of citizens temporarily abroad due to military threats.

Proper technological education of the participants in the process, representatives of the bar and the judiciary, and court employees is another intellectual challenge that electronic justice faces in modern conditions of the development of digital reality.

Keywords: e-justice, digitalization, digitalization, access to court, globalization, threats, justice, cyberattacks, national security, judicial system, war, legal regulation.