Когут В.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

ВІДЕОКОНФЕРЕНЦІЯ В СУДІ: ЗАБЕЗПЕЧЕННЯ ЛЕГІТИМНОСТІПРОЦЕСУ ТА ЗАХИСТ ВІД ДИПФЕЙКІВ

Цифрова трансформація судочинства в Україні, яка особливо активізувалася в період пандемії COVID-19 та під час воєнного стану, зумовила широке впровадження відеоконференцзв'язку як повноцінного інструменту правосуддя. Однак дистанційний формат судового провадження породжує низку проблем, пов'язаних із забезпеченням легітимності процесу, достовірності доказів та належної ідентифікації учасників. На мою думку, особливої гостроти ці питання набувають у світлі стрімкого розвитку технологій deepfake, які створюють реальну загрозу підміни особи або фальсифікації відеодоказів. Тому у своїй роботі я зосередилася на дослідженні правових та технічних механізмів забезпечення легітимності відеоконференції в суді та визначенні ефективних засобів захисту від дипфейків.

Передусім варто звернутися до правових засад. Відповідно до статті 336 Кримінального процесуального кодексу України (КПК), судове провадження може здійснюватися в режимі відеоконференції у разі неможливості безпосередньої участі учасника за станом здоров'я, необхідності забезпечення безпеки осіб, для забезпечення оперативності судового провадження, під час дії воєнного стану або карантину, а також з інших підстав, визначених судом достатніми [5]. Важливо, що учасник справи має право брати участь у засіданні в режимі відеоконференції як у приміщенні іншого суду, так і поза його межами з використанням власних технічних засобів. Як слушно зазначає І. Цибко, «дистанційне правосуддя перестало бути екзотикою — сучасні системи забезпечують не лише трансляцію звуку та зображення, а й захищені канали для конфіденційного спілкування адвоката з підзахисним прямо під час засідання» [11]. Саме ця остання можливість, як мені здається, створює найбільші ризики з точки зору безпеки, оскільки знімає контроль суду за технічним середовищем учасника.

Аналізуючи практику використання відеоконференцій, можна виокремити як переваги, так і суттєві недоліки [3, 1]. До переваг, безперечно, належать: оперативність та економія ресурсів; зниження ризиків для свідків та потерпілих завдяки їх дистанційній участі; можливість залучення сторін з інших регіонів або держав; забезпечення безперервності судового процесу в умовах воєнного стану чи пандемії [4,

13]. Водночас, як свідчить вивчена мною література та судова практика, існують і ризики: технічна неможливість участі або переривання зв'язку (що, до речі, покладається на учасника, який подав заяву про участь у ВКЗ) [2]; проблеми з дотриманням принципів змагальності та рівності сторін; а головне – ризики підміни особи або фальсифікації доказів за допомогою технологій штучного інтелекту.

Окремо слід зупинитися на загрозах, пов'язаних із deepfake. Сучасні технології досягли такого рівня, що відрізнити справжній відеозапис від згенерованого стає майже неможливим без спеціальних засобів. У судовому контексті дипфейки створюють дві основні категорії загроз: по-перше, це можливість підміни особи учасника відеоконференції (підозрюваного, свідка, експерта), що ставить під сумнів саму легітимність процесу; по-друге, це ризик подання сфальсифікованих відеодоказів, що може призвести до судових помилок та порушення прав людини. Я переконана, що у 2025–2026 роках це питання набуває особливої актуальності, оскільки deepfake-відео можуть використовуватися для маніпулювання громадською думкою, шантажу або дискредитації учасників процесу.

Ключовим елементом забезпечення довіри до дистанційного правосуддя, на мій погляд, є надійна ідентифікація та автентифікація учасників. Відповідно до Закону України від 23 травня 2024 року № 3755-IX, «суд, який забезпечує проведення відеоконференції, зобов'язаний перевірити явку та встановити особи тих, хто з'явився, а також перевірити повноваження представників» [10, 9]. Підтвердження особи учасника відбувається шляхом його авторизації в системі із застосуванням електронного цифрового підпису (ЕЦП). Однак, як показує практика, ЕЦП не є абсолютним захистом від deepfake-підмін. Дослідники застерігають, що «чинне українське законодавство не містить спеціальних норм щодо допустимості доказів, отриманих із застосуванням ШІ, зокрема результатів автоматизованого розпізнавання облич або інших біометричних ідентифікацій» [6], тому доцільним видається використання багатофакторної автентифікації та біометричних методів верифікації (зокрема, аналіз райдужної оболонки ока). Суд, який забезпечує проведення відеоконференції, зобов'язаний перевірити явку та встановити особи тих, хто з'явився, а також перевірити повноваження представників – це беззаперечно, але чи достатньо цього в умовах сучасних технологій?

Щодо технологічних рішень для захисту від дипфейків, то ефективна протидія передбачає комплексний підхід. Узагальнюючи прочитане, можна виокремити чотири ключові напрями: по-перше, передові технології виявлення (алгоритми, що аналізують цифрові відбитки, нерівномірність освітлення, аномалії текстури шкіри, особливості дихання); по-друге, технології цифрового маркування контенту (цифрові водяні знаки, технологія блокчейн для підтвердження автентичності); по-третє, стратегічні ініціативи та співпраця між

цифровими платформами, технологічними компаніями та урядами; по-четверте, правове регулювання та громадська освіта щодо розпізнавання фейкового контенту [12]. На мій погляд, для судової системи найбільш перспективними є перші два напрями.

На завершення хотілося б окреслити шляхи вдосконалення правового регулювання. Я вважаю, що для мінімізації ризиків, пов'язаних з використанням deepfake у судочинстві, необхідно: закріпити на законодавчому рівні вимоги до використання засобів біометричної верифікації учасників відеоконференцій; запровадити обов'язкове застосування технологій цифрового маркування (цифрових водяних знаків) для відеозаписів судових засідань; розробити доступні процедури судової експертизи відеоматеріалів на предмет їх автентичності; забезпечити функціонування захищених каналів зв'язку для конфіденційного спілкування адвоката з підзахисним під час відеоконференції. Як зазначає О. Машталяр, «для збалансування інноваційних можливостей ШІ з гарантіями прав людини потрібен комплексний підхід – від визначення процесуального статусу даних, згенерованих ШІ, до впровадження критеріїв перевірки їх достовірності через експертну оцінку, валідацію методів тощо» [6].

Підсумовуючи, зазначу: відеоконференція є невід'ємним елементом сучасного цифрового правосуддя, який забезпечує доступність, оперативність та безпеку судового процесу. Однак, поряд з очевидними перевагами, дистанційний формат створює нові виклики, пов'язані з ризиками deepfakeпідмін та фальсифікації доказів. Забезпечення легітимності відеоконференції в суді потребує комплексного підходу, який поєднує правові, організаційні та технологічні механізми: від багатофакторної автентифікації учасників та використання цифрових водяних знаків до запровадження процедур судової експертизи відеоматеріалів. Подальший розвиток законодавства у цій сфері має бути спрямований на створення ефективної системи захисту прав учасників судового процесу в умовах цифрової трансформації правосуддя.

ЛІТЕРАТУРА:

1. Главюк І.В., Дроздов О.М. Проведення судового засідання у режимі відеоконференції у кримінальному провадженні: доктринальні та практичні проблеми. *Юридичний науковий електронний журнал*. 2023. № 1. С. 438–443.

2. Ефективність та складнощі відеоконференцій в судових процесах : матеріали заходу з підвищення професійного рівня адвокатів / Тетяна Рабко ; Вища школа адвокатури НААУ. –20.08.2025. – URL: https://www.hsa.org.ua/blog/efektivnist-taskladnoshhi-videokonferencii-v-sudovix-procesax1

3. Жовтан Ю. Використання відеоконференцзв'язку у кримінальному процесі: плюси та недоліки. *Юридична Газета*. URL:

https://yur-gazeta.com/dumka-eksperta/vikoristannya-videokonferenczvyazkuu-kriminalnomu-procesi-plyusi-ta-nedoliki.html

4. Колесніков А. П. Особливості запровадження та взаємодії модулів єдиної судової інформаційно-телекомунікаційної системи. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка*. 2024. Вип. 2 (106), ч. 1. С. 71–81.

5. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17

6. Машталяр О.М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2025. Випуск 92. Ч. 3. С. 276–282.

7. Морозов Є. Щодо проведення судового засідання у режимі відеоконференції. ADVOKAT POST. URL: https://advokatpost.com/shchodo-provedennia-sudovoho-zasidannia-urezhymi-videokonferentsii-advokat-ievhen-morozov/

8. Правила відеофіксації в суді: роз'яснення суддям, прокурорам, адвокатам, юристам, ЗМІ, вільним слухачам / ГО «Відкрита Україна». – Безоплатна правнича допомога. URL: https://legalaid.gov.ua/novyny/pravyla-videofiksatsiyi-v-sudi-roz-yasnennyasuddyam-prokuroram-advokatam-yurystam-zmi-vilnym-sluhacham/

9. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України та Кодексу адміністративного судочинства України щодо вдосконалення участі у судовому засіданні в режимі відеоконференції: Закон України від 23.05.2024 № 3755-IX. URL: https://zakon.rada.gov.ua/laws/show/3755-20#Text

10. Проведення процесуальних дій у режимі відеоконференції під час кримінального провадження. – WikiLegalAid. – URL: https://legalaid.wiki/index.php/Проведення_процесуальних_дій_у_режимі_відеоконференції_під_час_кримінального_провадження

11. Цибко І. Цифровізація кримінального процесу у судовій практиці: тенденції та виклики / Ірина Цибко // Юридична Газета. – 19.02.2026. – URL: https://yurgazeta.com/publications/practice/kriminalne-pravo-ta-proces/cifrovizaciyakriminalnogo-procesu-u-sudoviy-praktici-tendenciyi-ta-vikliki.html

12. Чотири стовпи захисту від діпфейків. StopFake. URL: https://www.stopfake.org/uk/chotiri-stovpi-zahistu-vid-dipfejkiv/

13. Чудик Н.О., Колесніков А.П., Канюка В.Є. Інституційно-правові детермінанти модернізації єдиної судової інформаційно-телекомунікаційної системи в умовах цифрової трансформації правосуддя. *Актуальні проблеми правознавства*. 2025. № 1. С. 55-61