СУДОУСТРІЙ; ПРОКУРАТУРА ТА АДВОКАТУРА

УДК 347.965
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/51

Деревянко Н. З.
https://orcid.org/0000-0002-4749-6782
Центр українсько-європейського міжнародного співробітництва

Полюшко А. М.
https://orcid.org/0009-0000-5343-2876

АДВОКАТСЬКА ТАЄМНИЦЯ В ЦИФРОВУ ЕПОХУ: ТРАНСФОРМАЦІЯ ЗМІСТУ, МЕЖ ТА МЕХАНІЗМІВ ПРАВОВОГО ЗАХИСТУ

У статті досліджено трансформацію змісту, меж і механізмів правового захисту адвокатської таємниці в умовах цифровізації юридичної професії та розвитку сучасних інформаційних технологій. Обґрунтовано, що цифрове середовище змінює не лише форму існування конфіденційної інформації, а й традиційні підходи до визначення предмета адвокатської таємниці, її просторових і технологічних меж та способів забезпечення. Встановлено розширення предмета адвокатської таємниці за рахунок метаданих документів і повідомлень, цифрових слідів професійної та процесуальної активності адвоката, інформації у хмарних сховищах, історії комунікації в месенджерах, журналів доступу до інформаційних систем, а також матеріалів, створених або опрацьованих із застосуванням технологій штучного інтелекту.

Розкрито вплив мультиплатформності зберігання інформації, використання сторонніх цифрових сервісів та поєднання професійного й приватного цифрового середовища адвоката на традиційне розуміння меж професійної конфіденційності. Проаналізовано основні ризики цифрового середовища, пов'язані з несанкціонованим доступом до адвокатсько-клієнтської комунікації, цифровим стеженням, форензичним дослідженням електронних носіїв та використанням штучного інтелекту.

Особливу увагу приділено еволюції практики Європейського суду з прав людини – від захисту професійного приміщення адвоката до поширення гарантій статті 8 Конвенції на електронні дані та цифрову комунікацію. Визначено концептуальне значення рішення у справі «Černý and Others v. the Czech Republic», яким фактично утверджено наскрізний характер захисту адвокатсько-клієнтської комунікації незалежно від того, на чиєму пристрої зберігається відповідна інформація. Показано значення цього стандарту для оцінки достатності процесуальних гарантій в Україні.

Встановлено, що українське законодавство, визнаючи електронну інформацію складовою адвокатської таємниці, не забезпечує цілісної спеціальної процедури раннього виявлення, відокремлення та недопущення використання привілейованих матеріалів під час форензичного дослідження цифрових носіїв. Наголошено також на необхідності нормативного опрацювання використання штучного інтелекту в адвокатській діяльності та уніфікації технічних стандартів конфіденційного спілкування під час дистанційного судочинства.

Обґрунтовано трирівневу модель забезпечення адвокатської таємниці, що передбачає узгоджене застосування правових, організаційних і технічних механізмів. Зроблено висновок, що ефективний захист професійної конфіденційності у цифрову епоху потребує переходу

© Деревянко Н. З., Полюшко А. М., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

від переважно формальних заборон неправомірного доступу до превентивної моделі, здатної запобігти самому ознайомленню з привілейованою інформацією до вирішення питання про допустимість такого доступу.

Ключові слова: *адвокатська таємниця, адвокатура, професійна конфіденційність, цифрові дані, електронні докази, штучний інтелект, цифрова безпека, практика ЄСПЛ.*

Постановка проблеми. Цифровізація адвокатської діяльності істотно змінює умови реалізації одного з базових інститутів професійної правничої допомоги – адвокатської таємниці. Якщо традиційно її захист пов'язувався передусім із конфіденційністю особистого спілкування, недоторканністю адвокатського досьє та професійного приміщення, то сучасне інформаційне середовище переносить значну частину адвокатсько-клієнтської комунікації у цифровий простір. Електронні документи, месенджери, хмарні сервіси, системи електронного судочинства, віддалені формати роботи та інструменти штучного інтелекту створюють нові способи зберігання, передавання й обробки інформації, водночас породжуючи додаткові ризики її несанкціонованого розкриття.

Аналіз останніх досліджень і публікацій. Особливої актуальності проблема набуває у зв'язку з тим, що цифрові дані не обмежуються конкретним фізичним носієм і можуть одночасно існувати на декількох пристроях, у резервних копіях та зовнішній інформаційній інфраструктурі. Це ускладнює визначення меж адвокатської таємниці та вимагає переосмислення традиційного підходу, заснованого на фізичному контролі адвоката над інформацією.

Додаткового значення набуває новітня практика Європейського суду з прав людини, яка послідовно поширює гарантії професійної конфіденційності на електронні дані та цифрові засоби комунікації. Рішення у справі «Černý and Others v. the Czech Republic» сформувало важливий орієнтир щодо необхідності спеціальних процедур ідентифікації та відокремлення привілейованих матеріалів незалежно від того, на чиєму пристрої вони зберігаються.

Водночас українське законодавство, визнаючи електронну інформацію складовою адвокатської таємниці, ще не забезпечує цілісної моделі її захисту під час вилучення, копіювання, форензичного дослідження та використання цифрових даних. Саме розрив між нормативним визнанням конфіденційності та реальними механізмами її забезпечення зумовлює необхідність комплексного наукового переосмислення змісту, меж і способів захисту адвокатської таємниці у цифрову епоху.

Постановка завдання. Мета статті полягає у комплексному дослідженні трансформації змісту, меж і механізмів правового захисту адвокатської таємниці в умовах цифровізації, визначенні основних ризиків для професійної конфіденційності та обґрунтуванні напрямів удосконалення правових, організаційних і технічних гарантій її забезпечення з урахуванням новітньої практики Європейського суду з прав людини.

Виклад основного матеріалу. Відповідно до статті 22 Закону України «Про адвокатуру та адвокатську діяльність» адвокатською таємницею є будь-яка інформація, що стала відома адвокату про клієнта, питання, з яких він звертався, зміст наданих порад і консультацій, складені адвокатом документи, інформація на електронних носіях та інші відомості, одержані під час здійснення адвокатської діяльності [1]. Кримінальний процесуальний кодекс України, своєю чергою, формує процесуальний вимір захисту такої інформації, забороняючи допит захисника як свідка щодо обставин, які стали йому відомі у зв'язку з виконанням функцій захисника, а також відомостей, що становлять адвокатську таємницю [2]. Відповідні гарантії закріплено й у Правилах адвокатської етики, у яких збереження конфіденційності постає не лише як юридичний обов'язок адвоката, а й як одна з фундаментальних етичних засад професії [3].

Показово, що законодавча дефініція адвокатської таємниці вже безпосередньо охоплює інформацію на електронних носіях [1]. Водночас саме по собі нормативне визнання цифрової форми інформації ще не означає належної адаптації механізмів її захисту до технологічних реалій. Електронні дані можуть бути дистанційно отримані або скопійовані без відома їх володільця, одночасно зберігатися на декількох пристроях та у хмарних середовищах, а під час форензичного дослідження нерідко виникає складність відокремлення інформації, охопленої професійною таємницею, від загального масиву цифрових даних. У доктрині адвокатську таємницю традиційно розглядають крізь єдність її предмета, суб'єктного складу та меж дії [4, с. 235]. Саме цифровізація найбільш відчутно трансформує перший і третій із цих елементів, поступово позбавляючи визначального значення традиційні просторові орієнтири

на кшталт «офісу адвоката», «особистої розмови» чи «паперового досьє».

У цифровому середовищі предмет адвокатської таємниці об'єктивно розширюється за рахунок категорій інформації, які попередня правова доктрина враховувала лише опосередковано. До них належать метадані документів і повідомлень, історія комунікації в месенджерах, вміст хмарних сховищ, журнали доступу до інформаційних систем, а також матеріали, створені або опрацьовані із використанням інструментів штучного інтелекту. І. Гордусь звертає увагу на те, що значна частка витоків конфіденційної інформації – за його оцінкою, близько 60 відсотків – пов'язана саме з людським фактором, зокрема з неналежним поводженням із метаданими офісних документів [5]. Ю. С. Григоренко звертає увагу на необхідність вироблення єдиних стандартів використання штучного інтелекту в адвокатській діяльності та формування технологічної компетентності адвоката як складової належної професійної правничої допомоги [6, с. 352]. Особливої обережності потребує використання загальнодоступних систем штучного інтелекту під час роботи з матеріалами справи, оскільки воно може створювати додаткові ризики для конфіденційності інформації та потребує належної професійної верифікації отриманих результатів.

Подібна трансформація відбувається й у зв'язку з розвитком електронного судочинства – функціонуванням Єдиної судової інформаційно-телекомунікаційної системи, використанням електронних адвокатських запитів із кваліфікованим електронним підписом, електронних ордерів та інших цифрових інструментів професійної взаємодії. За таких умов правове значення може мати вже не лише зміст документа чи повідомлення, а й сам цифровий слід професійної та процесуальної активності адвоката, здатний опосередковано розкривати відомості про клієнта, характер правової допомоги, стратегію захисту або інші дані, що підлягають конфіденційному режиму [6, с. 353]. Відтак цифровізація змінює не тільки обсяг інформації, охопленої адвокатською таємницею, а й саму логіку визначення її меж: конфіденційна комунікація дедалі частіше розподіляється між різними платформами, пристроями та інформаційними середовищами, що особливо виразно проявляється у використанні месенджерів, хмарних сервісів і технологій штучного інтелекту.

Традиційне розуміння меж адвокатської таємниці значною мірою ґрунтувалося на фізичному контролі адвоката над інформацією та носіями, на яких вона зберігалася. Цифрове середовище істотно змінює цю логіку щонайменше у трьох взаємопов'язаних аспектах. По-перше, формується мультиплатформність зберігання даних: одна й та сама інформація може одночасно існувати на пристрої адвоката, пристрої клієнта, у хмарному сховищі, резервній копії та кеші відповідного застосунку. У цьому контексті показовою є позиція ЄСПЛ у справі «Černý and Others v. the Czech Republic», яка засвідчує, що обсяг гарантій конфіденційності не повинен визначатися виключно технічним способом або місцем зберігання інформації [7].

По-друге, дедалі менш виразною стає межа між особистою та професійною цифровою комунікацією. Використання загальнодоступних месенджерів призводить до того, що інформація, яка може становити адвокатську таємницю, обробляється в інформаційній інфраструктурі приватних технологічних компаній, а рівень її фактичної захищеності залежить не лише від поведінки адвоката, а й від архітектури відповідного сервісу, застосованих протоколів шифрування, правил резервного копіювання та політик зберігання метаданих. Саме тому практико-орієнтовані джерела наголошують на доцільності використання каналів комунікації із наскрізним шифруванням та інших засобів мінімізації ризику несанкціонованого доступу [5; 8].

По-третє, розмивається межа між професійним і приватним цифровим середовищем самого адвоката. Один і той самий ноутбук, смартфон або планшет нерідко використовується як для роботи з матеріалами справи та спілкування з клієнтами, так і для особистого листування, доступу до соціальних мереж чи інших сервісів. Водночас професійна діяльність дедалі частіше здійснюється поза межами традиційного офісу – із домашніх мереж, під час відряджень, у коворкінгах або із використанням публічних точок доступу до мережі Інтернет [9; 10]. За таких умов конфіденційність перестає бути лише питанням охорони окремого документа чи приміщення і набуває характеру постійного режиму захисту цифрового середовища професійної діяльності адвоката.

Окремий вимір проблеми становлять загрози, пов'язані не з випадковою втратою даних, а з цілеспрямованим доступом до професійної комунікації. У звіті організації Lawyers for Lawyers «Lawyer-Client Confidentiality in a Digitalized Society» виокремлено три основні категорії таких ризиків: цільове цифрове стеження за адвокатами із використанням шпигунського програм-

ного забезпечення, здатного забезпечити доступ до конфіденційних матеріалів і стратегії захисту; випадкове або цілеспрямоване отримання привілейованої інформації органами розслідування за відсутності належних процедур її ідентифікації та відокремлення; а також системне перехоплення комунікацій у межах програм масового спостереження [11]. Для української правової системи ці ризики набувають особливої актуальності в умовах повномасштабної збройної агресії, коли об'єктивне посилення безпекової складової діяльності держави має поєднуватися із збереженням належних гарантій конфіденційності професійної правничої допомоги.

Отже, цифровізація змінює не лише технічні способи зберігання та передавання інформації, а й самі критерії, за якими визначаються межі допустимого втручання у конфіденційну комунікацію адвоката і клієнта. Відповідно, особливого значення набуває еволюція підходів Європейського суду з прав людини, у практиці якого поступово сформувалося розширене розуміння професійної конфіденційності – від захисту адвокатського офісу та кореспонденції до охорони цифрових носіїв, електронних комунікацій і пов'язаних із ними даних.

Практика Європейського суду з прав людини щодо захисту адвокатської таємниці формувалася послідовно, поступово розширюючи розуміння сфери дії статті 8 Конвенції про захист прав людини і основоположних свобод. Однією з вихідних у цьому процесі стала справа «Niemietz v. Germany», у якій Суд поширив гарантії статті 8 на професійне приміщення адвоката та визнав, що його обшук становить втручання у право на повагу до приватного життя, житла та кореспонденції [12]. Цей підхід отримав подальший розвиток у справі «Roemen and Schmit v. Luxembourg», у якій ЄСПЛ визнав непропорційним обшук офісу адвоката, проведений у межах розслідування, спрямованого на встановлення журналістського джерела її клієнта, наголосивши на особливому значенні процесуальних гарантій під час втручання у сферу професійної конфіденційності [13]. У справі «Wieser and Bicos Beteiligungen GmbH v. Austria» відповідні стандарти було поширено на електронні дані, доступ до яких отримано під час обшуку, що стало важливим етапом адаптації гарантій статті 8 Конвенції до цифрового середовища [14]. У справі «Kolesnichenko v. Russia» Суд наголосив на необхідності достатнього обґрунтування втручання та існування ефективних гарантій від невиправданого доступу до інформації, охопленої професійною таємницею адвоката [15]. Окрему лінію практики становлять рішення щодо конфіденційності спілкування адвоката з клієнтом, який перебуває під вартою, у яких можливість приватного спілкування із захисником розглядається як важлива складова ефективної правової допомоги та справедливого судового розгляду.

Новий етап у розвитку цих стандартів позначило рішення у справі «Černý and Others v. the Czech Republic» від 18 грудня 2025 року [16; 7]. Під час кримінального провадження щодо клієнта правоохоронні органи вилучили його смартфон і планшет, після чого шляхом форензичного копіювання отримали значний масив цифрових даних – понад двадцять тисяч сторінок матеріалів, серед яких містилося конфіденційне листування клієнта з п'ятьма адвокатами, проєкти процесуальних документів, нотатки щодо стратегії захисту та інша професійно привілейована інформація. Ці матеріали були включені до кримінального провадження та стали доступними стороні обвинувачення й іншим учасникам процесу. ЄСПЛ констатував порушення статті 8 Конвенції, оскільки національне правове регулювання не забезпечувало достатньо чіткої та передбачуваної процедури ідентифікації, відбору та відокремлення привілейованих матеріалів, отриманих з вилучених електронних пристроїв. Водночас було встановлено й порушення статті 13 у поєднанні зі статтею 8, адже ефективний засіб правового захисту в таких обставинах повинен дозволяти не лише отримати компенсацію постфактум, а й домогтися вилучення з матеріалів провадження або знищення незаконно отриманої конфіденційної інформації [16].

Концептуальне значення рішення «Černý and Others v. the Czech Republic» полягає насамперед у переході від захисту конкретного фізичного носія до захисту самої природи адвокатсько-клієнтської комунікації. ЄСПЛ фактично виходить із того, що спеціальна охорона такого спілкування втратила б практичний зміст, якби поширювалася лише на інформацію, що зберігається безпосередньо на пристроях адвоката, але припиняла діяти щодо тієї самої комунікації після її збереження на пристрої клієнта [7]. Отже, визначальним стає не місце фізичного знаходження електронного носія і не особа, у володінні якої він перебуває, а зміст і характер відповідної інформації. Такий підхід надає захисту адвокатської таємниці своєрідного наскрізного характеру та істотно посилює її значення у цифровому середовищі.

Для України цей стандарт має особливе практичне значення, оскільки вилучення та дослідження смартфонів, комп'ютерів та інших цифрових носіїв у межах кримінального провадження потенційно відкриває доступ не лише до інформації, яка має доказове значення, а й до значних масивів адвокатсько-клієнтської комунікації. Відтак національне процесуальне регулювання потребує оцінки вже не тільки з позицій формальної заборони доступу до адвокатської таємниці, а й з погляду наявності дієвої процедури раннього виявлення, відокремлення та недопущення використання привілейованих цифрових даних. Саме у цьому аспекті стандарт, сформований у справі «Černý and Others v. the Czech Republic», створює нову нормативну оптику для аналізу достатності передбачених українським законодавством гарантій.

Законодавство України, попри формальне включення інформації на електронних носіях до предмета адвокатської таємниці, не формує цілісного процесуального механізму, який повною мірою відповідав би стандарту, сформованому у справі «Černý and Others v. the Czech Republic». Передбачена статтею 65 Кримінального процесуального кодексу України заборона допиту захисника щодо відомостей, які стали йому відомі у зв'язку з виконанням професійних функцій [2], спрямована передусім на недопущення безпосереднього отримання такої інформації від самого адвоката. Водночас цифрове середовище створює інший, опосередкований канал доступу до привілейованих відомостей – шляхом форензичного дослідження пристроїв, вилучених у клієнта, інших учасників провадження чи третіх осіб. Саме на цьому етапі традиційні гарантії адвокатської таємниці виявляються найменш пристосованими до технологічної природи сучасних доказів.

Процесуальні правила проведення обшуку, тимчасового доступу та вилучення електронних інформаційних систем і носіїв не передбачають спеціальної універсальної процедури попередньої ідентифікації та відокремлення адвокатсько-клієнтської комунікації під час подальшого аналізу отриманого масиву даних. Особливої ваги набуває те, що процесуальна дія фактично не завершується фізичним вилученням пристрою: основне втручання у сферу конфіденційності нерідко відбувається вже на стадії створення цифрової копії, пошуку за ключовими словами, відновлення видалених файлів та аналізу листування. У справі «Golovan v. Ukraine» ЄСПЛ уже наголошував на значенні належних незалежних гарантій під час проведення процесуальних дій, здатних зачіпати адвокатську таємницю [17]. У цифровому середовищі ця проблема набуває якісно іншого масштабу, оскільки один смартфон, ноутбук або образ накопичувача може містити величезний масив різнорідної інформації, у якому професійно привілейовані матеріали співіснують із даними, що не мають жодного стосунку до адвокатської діяльності. Без спеціально визначеної процедури їх відокремлення сам факт правомірного доступу до носія ще не гарантує правомірності доступу до всього його вмісту.

Ситуацію ускладнює й те, що чинне процесуальне регулювання не повною мірою враховує специфіку збирання, копіювання, дослідження та оцінки цифрових даних, особливо коли їх опрацювання здійснюється із застосуванням автоматизованих інструментів або технологій штучного інтелекту. У цьому контексті проблема полягає не стільки у відсутності загальних правил допустимості доказів, скільки у недостатній деталізації спеціальних гарантій, здатних забезпечити збереження привілейованої інформації на всіх етапах роботи з цифровим масивом. Адже технологічна можливість швидко проаналізувати значні обсяги даних істотно посилює ризик того, що доступ до інформації, яка не мала бути предметом дослідження, відбудеться ще до того, як буде вирішено питання про її процесуальний статус.

Окремого значення проблема адвокатської таємниці набуває в умовах дистанційного здійснення правосуддя, поширення якого особливо посилилося в період воєнного стану. М. А. Погорецький, аналізуючи зміни кримінального процесуального законодавства цього періоду, звертає увагу на те, що дистанційна участь підозрюваного у судовому засіданні повинна поєднуватися із реальною можливістю конфіденційного спілкування із захисником, посилаючись, зокрема, на підходи ЄСПЛ у справі «Marcello Viola v. Italy» щодо необхідності забезпечення ефективної участі обвинуваченого та взаємодії із захисником. Формального надання засобу відеозв'язку для цього недостатньо: конфіденційність має забезпечуватися і технічно, і організаційно – таким чином, щоб сторонні особи не могли чути зміст консультації, а використовувані канали зв'язку не створювали невиправданого ризику її перехоплення або запису. Водночас відсутність уніфікованих обов'язкових технічних стандартів залишає значний простір для різної практики окремих судів, установ виконання покарань та інших органів [18, с. 254; 19].

Таким чином, цифрова трансформація виявляє системну особливість чинної моделі захисту адвокатської таємниці: більшість її гарантій сформу-

льовано як заборони неправомірного доступу до конфіденційної інформації, тоді як цифрове середовище потребує ще й процедур, здатних запобігти самому ознайомленню з привілейованими даними до вирішення питання про допустимість такого доступу. Саме тому подальший розвиток правового регулювання має бути пов'язаний не лише з уточненням обсягу адвокатської таємниці, а передусім із побудовою спеціальних превентивних механізмів її захисту на стадіях вилучення, копіювання, аналізу, зберігання та використання цифрової інформації.

Ефективний захист адвокатської таємниці в цифрову епоху потребує системного поєднання правових, організаційних і технічних механізмів. На правовому рівні першочергового значення набуває законодавче закріплення спеціальної процедури виявлення, відбору та відокремлення матеріалів, що можуть становити адвокатську таємницю, під час вилучення та подальшого форензичного дослідження електронних носіїв. Така процедура має передбачати незалежний механізм перевірки привілейованого характеру інформації, можливість оперативного заперечення проти її дослідження чи використання, а також чіткий порядок вилучення відповідних матеріалів із доказового масиву та їх подальшого знищення або повернення. Саме відсутність ефективної процедури ідентифікації та відокремлення привілейованих цифрових даних стала одним із ключових чинників констатації порушення статей 8 і 13 Конвенції у справі «Černý and Others v. the Czech Republic» [16]. Окремого нормативного опрацювання потребують і питання використання штучного інтелекту під час підготовки та аналізу юридично значущої інформації, зокрема межі допустимого застосування таких технологій, вимоги до професійної верифікації отриманих результатів та відповідальність за неналежне поводження з конфіденційними даними. Не менш важливим є встановлення уніфікованих вимог до дистанційного судочинства, які забезпечували б реальну, а не лише формальну можливість конфіденційного спілкування адвоката з клієнтом.

На організаційному рівні захист адвокатської таємниці передбачає формування внутрішніх політик кібербезпеки та цифрової гігієни, що охоплювали б регулярне оновлення програмного забезпечення, розмежування прав доступу до інформаційних систем, контроль операцій із конфіденційними матеріалами, резервне копіювання даних, а також систематичне навчання адвокатів і працівників адвокатських бюро та об'єднань. З огляду на істотну роль людського фактора у виникненні витоків конфіденційної інформації, доцільним видається розроблення Національною асоціацією адвокатів України мінімальних стандартів цифрової безпеки адвокатської діяльності. Такі стандарти могли б конкретизувати загальний обов'язок зі збереження адвокатської таємниці, передбачений статтею 22 Закону України «Про адвокатуру та адвокатську діяльність» [1], адаптуючи його до використання електронних засобів комунікації, хмарних сервісів, мобільних пристроїв та автоматизованих систем обробки інформації.

На технічному рівні належний захист передбачає застосування наскрізного шифрування комунікації з клієнтами, багатофакторної автентифікації, безпечних засобів керування паролями, шифрування файлів і резервних копій, захищених каналів доступу до інформаційних систем, а також очищення документів від метаданих перед їх передаванням третім особам. Використання хмарних сервісів із належним рівнем інформаційної безпеки та архітектурою, яка мінімізує можливість доступу постачальника послуг до змісту конфіденційних даних, також може істотно зменшувати ризики їх несанкціонованого розкриття. Водночас технічні засоби не повинні розглядатися як самодостатня гарантія, оскільки ефективність будь-якого інструменту залежить від належної організаційної дисципліни його використання та існування правових правил, які визначають допустимі межі доступу до захищеної інформації.

Отже, жоден із зазначених рівнів окремо не здатний забезпечити належний режим адвокатської таємниці у цифровому середовищі. Технічні рішення втрачають ефективність без організаційної культури безпеки, організаційні правила залишаються недостатніми без належних процесуальних гарантій, а правові заборони не забезпечують реального захисту без технологічних засобів, здатних запобігти несанкціонованому доступу до інформації. Саме системне поєднання цих елементів дозволяє перейти від формального проголошення конфіденційності до її реального забезпечення та відповідає загальному напряму розвитку стандартів ЄСПЛ, найбільш виразно відображеному у справі «Černý and Others v. the Czech Republic».

Висновки. Проведене дослідження засвідчує, що адвокатська таємниця в цифрову епоху зазнає глибокої змістовної та функціональної трансформації. Цифровізація змінює не лише форму існування конфіденційної інформації, а й самі підходи до визначення її предмета, меж та способів пра-

вового захисту. До традиційних відомостей про клієнта, зміст консультацій і стратегію захисту дедалі виразніше додаються метадані, цифрові сліди професійної та процесуальної активності, інформація, розміщена у хмарних середовищах, а також матеріали, створені чи опрацьовані із застосуванням систем штучного інтелекту. Водночас мультиплатформність зберігання даних, використання месенджерів і сторонніх цифрових сервісів, а також стирання межі між професійним і приватним інформаційним середовищем адвоката ускладнюють традиційне розуміння конфіденційності як контролю над конкретним документом, носієм або приміщенням.

Практика Європейського суду з прав людини відображає послідовний перехід від охорони фізичного простору адвокатської діяльності до захисту самої природи адвокатсько-клієнтської комунікації. Якщо у справі «Niemietz v. Germany» було закладено основу для поширення гарантій статті 8 Конвенції на професійне приміщення адвоката, то подальша практика поступово охопила електронні дані та цифрові засоби комунікації. Особливе значення в цьому контексті має рішення у справі «Černý and Others v. the Czech Republic», у якому підтверджено, що захист конфіденційного спілкування адвоката і клієнта не може залежати від того, на чиєму саме пристрої зберігаються відповідні електронні матеріали. Такий підхід фактично утверджує наскрізний характер адвокатської таємниці у цифровому середовищі й формує новий критерій оцінки достатності національних процесуальних гарантій.

Українське законодавство вже визнає електронну інформацію складовою адвокатської таємниці, однак механізми її практичного захисту залишаються недостатньо адаптованими до специфіки цифрових даних. Найбільш відчутними є відсутність спеціальної процедури раннього виявлення, відокремлення та недопущення використання привілейованих матеріалів під час форензичного дослідження електронних носіїв, недостатня деталізація правил роботи з цифровими даними із застосуванням автоматизованих систем і штучного інтелекту, а також неоднорідність технічних умов забезпечення конфіденційного спілкування під час дистанційного здійснення правосуддя. У зв'язку з цим подальше вдосконалення правового регулювання має орієнтуватися не лише на встановлення заборон неправомірного доступу до адвокатської таємниці, а й на створення превентивних процедур, здатних запобігти самому ознайомленню з привілейованою інформацією до вирішення питання про допустимість такого доступу.

Ефективна модель захисту адвокатської таємниці у цифровому середовищі повинна ґрунтуватися на взаємодії правових, організаційних і технічних механізмів. Правові гарантії мають визначати межі допустимого втручання та процесуальні наслідки їх порушення, професійні стандарти – формувати належну культуру цифрової безпеки, а технічні засоби – забезпечувати практичну стійкість конфіденційної комунікації та зберігання даних. Лише їх узгоджене функціонування здатне забезпечити перехід від формального визнання адвокатської таємниці до її реального захисту в умовах технологічної трансформації професії.

Перспективи подальших наукових досліджень доцільно пов'язувати з розробленням процесуальної моделі захисту привілейованих електронних матеріалів у кримінальному провадженні України, визначенням допустимих меж використання технологій штучного інтелекту в адвокатській діяльності та поглибленим порівняльно-правовим аналізом відповідних механізмів у державах – членах Європейського Союзу з урахуванням новітньої практики Європейського суду з прав людини.

Список літератури:

1. Про адвокатуру та адвокатську діяльність : Закон України від 5 липня 2012 р. № 5076-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/5076-17.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

3. Правила адвокатської етики : затверджені Звітно-виборним з'їздом адвокатів України 9 червня 2017 р. URL: https://zakon.rada.gov.ua/rada/show/n0001891-17.

4. Семенов М. В. Адвокатська таємниця: проблеми визначення предмету та обсягу. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 3. Ч. 3. С. 234–238. DOI: https://doi.org/10.24144/2788-6018.2025.03.3.35

5. Гордусь І. Захист адвокатської таємниці у цифрову епоху. Вища школа адвокатури НААУ. 2026. 9 січня. URL: https://www.hsa.org.ua/lectors/gordus-igor/articles/zaxist-advokatskoyi-tajemnici-u-cifrovu-epoxu1.

6. Григоренко Ю. С. Способи, прийоми та засоби захисту адвокатом прав клієнта в цифровому вимірі. *Соціально-політична та правова система України в цифрову епоху: сучасні виклики* : матеріали Міжна-

родної науково-практичної конференції. Одеса : Національний університет «Одеська юридична академія», 2026. Т. 1. С. 351–354.

7. Černý and Others v. the Czech Republic: A Step Forward in the Protection of Lawyer-Client Communications. ECHRCaseLaw. 2025. URL: https://www.echrcaselaw.com/en/echr-decisions/cerny-and-others-v-the-czech-republic-a-step-forward-in-the-protection-of-lawyer-client-communications/.

8. Winner. Адвокати у цифрову епоху: як захистити конфіденційність клієнтів. *Адвокати Захисники.* 2025. 26 квітня. URL: https://advocates.com.ua/lawyers-digital-era/.

9. Гордусь І. Основи цифрової безпеки для адвокатів. Вища школа адвокатури НААУ. 2025. 21 серпня. URL: https://www.hsa.org.ua/blog/osnovi-cifrovoyi-bezpeki-dlia-advokativ.

10. Рада В. Чому цифрова гігієна важлива для адвоката. RADAKO. Рада адвокатів Київської області. 2025. 5 серпня. URL: https://radako.com.ua/chomu-czyfrova-gigiyena-vazhlyva-dlya-advokata/.

11. Lawyers for Lawyers. Lawyer-Client Confidentiality in a Digitalized Society. 2023. May. URL: https://www.lawyersforlawyers.org/wp-content/uploads/2023/05/Lawyers-for-Lawyers-Digital-Lawyer-Client-Confidentiality.pdf.

12. European Court of Human Rights. Case of «Niemietz v. Germany» (Application no. 13710/88) : Judgment of 16 December 1992. *HUDOC*. URL: https://hudoc.echr.coe.int/eng?i=001-57887.

13. European Court of Human Rights. Case of «Roemen and Schmit v. Luxembourg» (Application no. 51772/99) : Judgment of 25 February 2003. *HUDOC*. URL: https://hudoc.echr.coe.int/fre?i=001-65515.

14. European Court of Human Rights. Case of «Wieser and Bicos Beteiligungen GmbH v. Austria» (Application no. 74336/01) : Judgment of 16 October 2007. *HUDOC*. URL: https://hudoc.echr.coe.int/eng?i=001-82711.

15. European Court of Human Rights. Case of «Kolesnichenko v. Russia» (Application no. 19856/04) : Judgment of 9 April 2009. *HUDOC*. URL: https://hudoc.echr.coe.int/eng?i=001-92147.

16. European Court of Human Rights. Case of «Černý and Others v. the Czech Republic» (Applications nos. 37514/20, 37525/20, 37533/20, 37546/20 and 37555/20) : Judgment of 18 December 2025. *HUDOC*. URL: https://hudoc.echr.coe.int/fre?i=001-247564.

17. European Court of Human Rights. Case of «Golovan v. Ukraine» (Application no. 41716/06) : Judgment of 5 July 2012. *HUDOC*. URL: https://hudoc.echr.coe.int/ukr?i=001-112021.

18. Погорецький М. А. Новели Кримінального процесуального кодексу України в період воєнного стану: проблемні питання. *Право і суспільство.* 2025. № 3. Т. 2. С. 248–262. DOI: https://doi.org/10.32842/2078-3736/2025.3.2.35.

19. European Court of Human Rights. Case of «Marcello Viola v. Italy» (Application no. 45106/04) : Judgment of 5 October 2006. *HUDOC*. URL: https://hudoc.echr.coe.int/eng?i=001-77246.

Derevianko N. Z., Polyushko A. M. LAWYER–CLIENT CONFIDENTIALITY IN THE DIGITAL AGE: TRANSFORMATION OF ITS SCOPE, BOUNDARIES, AND LEGAL PROTECTION MECHANISMS

The article examines the transformation of the content, boundaries, and legal protection mechanisms of lawyer–client confidentiality in the context of the digitalisation of the legal profession and the development of modern information technologies. It is argued that the digital environment alters not only the form in which confidential information exists, but also traditional approaches to defining the scope of lawyer–client confidentiality, its spatial and technological boundaries, and the means of ensuring its protection. The scope of protected information is shown to be expanding to include document and message metadata, digital traces of lawyers' professional and procedural activity, information stored in cloud environments, communication histories in messaging applications, access logs of information systems, as well as materials generated or processed with the use of artificial intelligence technologies.

The article explores how multi-platform data storage, reliance on third-party digital services, and the overlap between lawyers' professional and private digital environments affect the traditional understanding of professional confidentiality. The principal risks associated with the digital environment are analysed, including unauthorised access to lawyer–client communications, digital surveillance, forensic examination of electronic devices, and the use of artificial intelligence.

Particular attention is paid to the evolution of the case-law of the European Court of Human Rights, from the protection of lawyers' professional premises to the extension of the guarantees under Article 8 of the Convention to electronic data and digital communications. The conceptual significance of Černý and Others v. the Czech Republic is highlighted, as the judgment effectively affirmed the continuous nature of protection afforded to lawyer–client communications irrespective of whose device stores the relevant information. The importance of this standard for assessing the adequacy of procedural safeguards in Ukraine is demonstrated.

The article establishes that, although Ukrainian legislation recognises electronic information as falling within the scope of lawyer–client confidentiality, it does not provide a comprehensive special procedure for the early identification, segregation, and exclusion from use of privileged materials during the forensic examination of digital devices. The need for further regulation of the use of artificial intelligence in legal practice and for the harmonisation of technical standards governing confidential communication in remote judicial proceedings is also emphasised.

A three-level model for safeguarding lawyer–client confidentiality is substantiated, based on the coordinated application of legal, organisational, and technical mechanisms. It is concluded that effective protection of professional confidentiality in the digital age requires a shift from predominantly formal prohibitions on unlawful access towards a preventive model capable of preventing access to privileged information before the lawfulness and admissibility of such access have been determined.

Keywords: *lawyer–client confidentiality, legal profession, professional confidentiality, digital data, electronic evidence, artificial intelligence, digital security, ECtHR case-law.*

Дата першого надходження статті до видання: 04.09.2026
Дата прийняття статті до друку після рецензування: 18.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026