

ПАК О. В.,

orcid.org/0009-0008-3108-2236

аспірант кафедри цивільного права
та процесу

(Навчально-науковий інститут
№ 5 Харківського національного
університету внутрішніх справ)

УДК 347.44:004.738.5(100)

DOI <https://doi.org/10.32842/2078-3736/2025.6.15>

УДОКОНАЛЕННЯ ЦИВІЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ ОНЛАЙН-ТРЕНУВАНЬ З УРАХУВАННЯМ МІЖНАРОДНОГО ДОСВІДУ

Стаття присвячена комплексному аналізу удосконалення цивільно-правового регулювання онлайн-тренувань у контексті європейської інтеграції та формування єдиного цифрового ринку послуг. Досліджено правову природу договорів про надання онлайн-тренувальних послуг, визначено їх істотні умови, специфіку укладення та виконання в електронній і цифровій формах. Особлива увага приділена проблематиці встановлення належного волевиявлення сторін, застосуванню електронних підписів, методам автентифікації та верифікації користувачів, а також забезпеченню необхідного рівня захисту персональних і чутливих даних відповідно до сучасних європейських стандартів та вимог міжнародної цифрової безпеки.

Проаналізовано ключові ризики правозастосування, пов'язані з технічними збоями, нестабільністю доступу до цифрової платформи, недоліками тренувального контенту та особливостями цифрових доказів, включаючи лог-файли, журнали транзакцій, метадані та електронну комунікацію сторін. Показано, що відсутність достатньої правової визначеності у сфері онлайн-тренувань створює значні труднощі для судової практики, зокрема щодо ідентифікації сторін, встановлення факту порушення та доведення причинно-наслідкового зв'язку при наданні дистанційних послуг. Обґрунтовано необхідність гармонізації національного законодавства з актами ЄС у сфері цифрових послуг, електронної комерції та захисту споживачів, а також адаптації національних норм до вимог розвитку інноваційних моделей тренувального середовища.

На основі порівняльного аналізу зарубіжних підходів сформульовано пропозиції щодо удосконалення українського регулювання онлайн-тренувань, спрямовані на унормування діяльності цифрових платформ, уточнення меж відповідальності виконавця та користувача, посилення цифрової безпеки й формування довіри до електронних форм взаємодії.

Наголошено на важливості створення цілісної правової моделі, здатної забезпечити баланс інтересів споживачів, тренерів і постачальників цифрової інфраструктури.

Ключові слова: *онлайн-тренування, електронний договір, цивільно-правова відповідальність, цифрове регулювання, міжнародний досвід, захист споживачів, електронна комерція; персональні дані.*

Pak O. V. Improving civil law regulation of online training taking into account international experience

The article is devoted to a comprehensive analysis of the improvement of civil law regulation of online training in the context of European integration and the formation



of a single digital services market. The work examines the legal nature of contracts for the provision of online training services, their essential terms and features of their conclusion in electronic and digital forms. The emphasis is placed on the issues of determining the proper expression of the parties' will, the use of electronic signatures, user authentication and verification procedures, as well as ensuring an adequate level of protection of personal and sensitive data in accordance with modern European standards.

The key risks of law enforcement associated with technical failures, denials of access to the digital platform, content deficiencies and the specifics of digital evidence, in particular log files, transaction logs and electronic communication of the parties, are analyzed. The author substantiates the importance of legal certainty in the field of online training and the need to harmonize national legislation with the requirements of international acts, including the EU directives on digital services and e-commerce.

Particular attention is paid to foreign models of regulation of electronic contracts and consumer protection, which allows us to formulate proposals for improving the Ukrainian approach to the regulation of digital training services.

The need to establish clear rules for the functioning of online training services, standardize the mechanisms of responsibility of the performer and user, as well as strengthen digital security and trust in electronic forms of interaction is emphasized.

Key words: *online training, electronic contract, civil liability, digital regulation, international experience, consumer protection, e-commerce, personal data.*

Вступ. Стрімкий розвиток цифрових технологій, зростання ролі дистанційних сервісів та зміна моделей споживання послуг призвели до формування нового сегмента ринку – онлайн-тренувань, що охоплюють фізичні, освітні, консультаційні та оздоровчі практики, здійснювані через цифрові платформи. Така форма взаємодії значно спрощує доступ до тренувальних програм, забезпечує гнучкість та персоналізацію послуг, водночас створюючи низку правових викликів. Незважаючи на існування загальних норм цивільного законодавства та спеціальних актів у сфері електронної комерції, правова природа договорів про надання онлайн-тренувальних послуг залишається недостатньо визначеною, а механізми їх укладення та виконання – нерідко фрагментарними.

Особливої актуальності набувають питання встановлення належного волевиявлення сторін, ідентифікації споживача та виконавця, використання електронного підпису, технічної фіксації істотних умов договору, а також підтвердження факту його укладення у цифровій формі. В умовах цифровізації зростає роль належної обробки персональних даних, відеоматеріалів, результатів тренувань та індивідуальних консультацій, що, своєю чергою, потребує надійних правових механізмів захисту приватності та цифрової безпеки.

Додатковим фактором є міжнародна практика, яка демонструє високий рівень регулювання електронних договорів, споживчих прав та цифрових сервісів, що може бути корисним орієнтиром для вдосконалення українського законодавства. Відсутність єдиного підходу до кваліфікації договорів онлайн-тренувань спричиняє правову невизначеність, ускладнює захист прав учасників правовідносин та створює ризики для стабільності цивільного обороту.

В таких умовах виникає потреба у комплексному дослідженні договірних механізмів онлайн-тренувань, визначенні їх змісту й правової характеристики, а також у формуванні теоретичних та практичних підходів до вдосконалення цивільно-правового регулювання з урахуванням міжнародних стандартів цифрової взаємодії.

Постановка проблеми. Сучасний розвиток онлайн-тренувальних послуг вимагає визначення оптимальних підходів до їх правового регулювання, зокрема щодо укладення договорів у електронній та цифровій формах, забезпечення прозорості взаємодії між споживачем і виконавцем та належного рівня цифрової безпеки. У національному законодавстві



відсутні спеціальні норми, які комплексно врегульовують особливості таких договорів, що зумовлює необхідність ґрунтовного наукового аналізу та вироблення відповідних пропозицій.

У зв'язку з цим завданням статті є:

- з'ясувати правову природу договорів про надання онлайн-тренувальних послуг та їх місце в системі цивільно-правових зобов'язань;
- охарактеризувати особливості укладення таких договорів в електронній та цифровій формі, включно з питаннями ідентифікації сторін, електронного підпису та фіксації істотних умов;
- визначити основні ризики та проблеми правозастосування, пов'язані з технічними збоями, цифровими доказами, обробкою персональних даних та відповідальністю за порушення умов договору;
- здійснити порівняльно-правовий аналіз міжнародних підходів до регулювання електронних договорів та онлайн-послуг;
- сформулювати пропозиції щодо удосконалення цивільно-правового регулювання онлайн-тренувань з урахуванням міжнародного досвіду та потреб споживачів у безпечному цифровому середовищі.

Результати дослідження. Укладання договорів про надання онлайн-тренувальних послуг відбувається переважно в електронній та цифровій формі через веб-сайти, мобільні застосунки, платформи та месенджери. З погляду цивільного законодавства України, правочини, вчинені за допомогою інформаційно-телекомунікаційних систем, за умови дотримання вимог щодо ідентифікації сторін і фіксації їх волевиявлення, прирівнюються до письмової форми договору [7; 13]. Закон України «Про електронну комерцію» спеціально встановлює, що електронний правочин має таку ж юридичну силу, як і правочин у звичайній письмовій формі, за умови використання належних засобів електронної ідентифікації та збереження електронних доказів його вчинення [7; 8].

Ключовим елементом укладення таких договорів є ідентифікація сторін. У практиці онлайн-тренувань вона здійснюється через створення облікового запису, використання логіну й пароля, одноразових ідентифікаційних кодів, а також, за потреби, застосування засобів електронної ідентифікації підвищеного рівня довіри. Закон України «Про електронні довірчі послуги» запроваджує класифікацію електронних підписів (звичайний, удосконалений, кваліфікований) і закріплює презумпцію юридичної рівноцінності кваліфікованого електронного підпису власноручному підпису фізичної особи [6]. Це створює нормативну основу для використання кваліфікованих електронних підписів при укладенні договорів онлайн-тренувань, особливо в разі довгострокових, абонентських чи високоризикових зобов'язань.

Водночас у масовій споживчій практиці укладення таких договорів часто відбувається в спрощених моделях: шляхом проставлення «галочки» у полі «Я погоджуюсь з умовами договору», натискання кнопки «Підтвердити оплату», «Придбати абонемент» тощо (click-wrap, scroll-wrap-угоди). У світлі вимог Закону України «Про електронну комерцію» такі дії можуть розглядатися як акцепт публічної оферти чи індивідуальної пропозиції, за умови, що споживачу до моменту акцепту було надано доступ до повного тексту умов договору, інформації про виконавця, ціну, строк та інші істотні умови [7; 8].

Європейська практика також виходить із того, що договір вважається укладеним, якщо споживач чітко поінформований про умови і здійснив однозначну дію, що свідчить про згоду (підхід, закріплений у Директиві 2011/83/ЄС про права споживачів) [18].

Окремого аналізу потребує використання електронного підпису у сфері онлайн-тренувань. З одного боку, для більшості типових споживчих договорів достатнім є спрощений механізм підтвердження волевиявлення (обліковий запис, одноразові коди, підтвердження через e-mail або SMS), що відповідає концепції електронної ідентифікації, закріпленій у Регламенті (ЄС) № 910/2014 (eIDAS) [31]. З іншого боку, у разі виникнення спору щодо факту укладення договору чи змісту істотних умов саме застосування кваліфікованого електронного підпису значно підсилює позиції сторін з огляду на презумпцію достовірності



походження підпису та цілісності даних [6; 31]. У цьому контексті доцільною є диференціація вимог до електронного підпису залежно від вартості послуг, тривалості договору та рівня ризику обробки чутливих персональних даних.

Не менш важливою є проблема фіксації істотних умов договору. Для договорів онлайн-тренувань істотними, окрім предмета та ціни, є умови про тривалість програми, формат проведення занять (онлайн-сесії в реальному часі, відеозаписи, індивідуальні консультації), розклад, порядок доступу до цифрового контенту, правила відміни та перенесення занять, відповідальність сторін, а також положення про обробку персональних даних і конфіденційність [5; 13].

Закон України «Про електронну комерцію» вимагає, щоб суб'єкт електронної комерції забезпечував можливість збереження та відтворення електронних документів, пов'язаних з правочином, що є ключовим для подальшого доказування факту укладення договору й погодження істотних умов [7]. У європейському праві Директива (ЄС) 2019/770 щодо контрактів на надання цифрового контенту та цифрових послуг наголошує на необхідності чіткого визначення основних характеристик цифрового контенту та умов його постачання, включно з оновленнями і доступністю сервісу [16].

Сукупність цих вимог зумовлює потребу у належній організації електронного документообігу у сфері онлайн-тренувань. Йдеться про зберігання електронних логів (час входу в систему, акцепт оферти, оплати), копій електронних повідомлень, версій умов публічної оферти, політик конфіденційності та згод на обробку даних. Практика показує, що саме належно організований електронний архів стає основним джерелом доказів у разі виникнення спору щодо обсягу наданих послуг, дотримання графіку тренувань або правомірності обробки персональних даних [5; 7; 8].

Таким чином, особливості укладення договорів онлайн-тренувань в електронній та цифровій формі пов'язані, насамперед, із:

- 1) використанням спеціальних механізмів ідентифікації сторін та електронних підписів;
- 2) технічно зумовленими способами фіксації істотних умов договору;
- 3) вимогами до збереження цифрових доказів;
- 4) поєднанням договірних регулювань з вимогами у сфері захисту персональних даних і цифрового контенту.

Вирішення цих питань можливе лише на основі узгодженого застосування норм цивільного законодавства, спеціальних законів про електронну комерцію й електронні довірчі послуги, а також імплементації європейських стандартів, закріплених у актах ЄС щодо електронної ідентифікації та цифрових послуг [7; 6; 9; 10; 28; 31].

Технічні збої платформ, мобільних застосунків або серверної інфраструктури можуть призвести до неможливості проведення онлайн-занять чи доступу до цифрового контенту. У таких випадках виникає проблема визначення того, чи є збій порушенням зобов'язання виконавця, чи він спричинений зовнішніми обставинами, що можуть бути кваліфіковані як форс-мажор [10; 13].

Додатковою проблемою є відсутність у національному законодавстві чітких критеріїв для кваліфікації IT-збоїв як непереборної сили, тоді як міжнародна практика (зокрема в межах eIDAS та Digital Services Act) підкреслює важливість технічної надійності сервісу [30; 31].

Електронні докази – цифрові логи, історія платежів, листування в месенджерах, записи відеосесій – є основним інструментом доведення факту укладення й виконання договору. Закон України «Про електронну комерцію» вимагає забезпечення можливості збереження та відтворення електронних повідомлень [7], однак практичне застосування цієї норми ускладнене відсутністю єдиних стандартів фіксації та підтвердження автентичності цифрових доказів [8].

Судова практика також свідчить про проблеми з доведенням походження цифрових файлів і встановленням їх цілісності, що значно впливає на можливість довести факт порушення договору [19].



Онлайн-тренування передбачають обробку персональних і часто чутливих даних: відеоматеріалів, інформації про фізичний стан, фотографій, комунікацій між тренером і клієнтом. Закон України «Про захист персональних даних» та GDPR встановлюють суворі вимоги до згоди, безпеки зберігання та передачі персональних даних [9; 28].

Основні проблеми включають: – недостатню прозорість політик конфіденційності; використання нестабільних або небезпечних цифрових сервісів (Zoom, Instagram, Telegram); ризики витоку персональних відеозаписів; – відсутність чіткої згоди споживача на обробку даних, що може спричинити відповідальність виконавця [9].

Модель надання онлайн-тренувальних послуг часто включає кількох учасників: тренера, платформу, платіжну систему, хмарний сервіс. Це створює труднощі у визначенні відповідальності за порушення, зокрема: неможливість провести тренування через збій платформи; помилкові автоматичні списання коштів; надання тренером некоректних рекомендацій, що можуть завдати шкоди здоров'ю; невиконання умов щодо повернення коштів при достроковому припиненні підписки [10; 13].

Європейська Директива 2019/770 передбачає стандарти щодо цифрових послуг та відповідальності за невідповідність цифрового контенту, однак у національному праві аналогічні механізми залишаються недостатньо розвиненими [16]. Це створює прогалини в правозастосуванні та обмежує можливості ефективного захисту прав споживачів.

Правозастосування у сфері договорів онлайн-тренувань характеризується підвищеним рівнем цифрових ризиків, що зумовлені технічною природою надання послуги та недостатньою деталізацією законодавства. Вони впливають як на можливість належного виконання договору, так і на подальший захист прав сторін.

Онлайн-тренування здійснюються через спеціалізовані цифрові платформи, які є вразливими до технічних збоїв: проблем із серверами, нестабільності інтернет-з'єднання, збоїв у роботі програмного забезпечення, кіберінцидентів тощо. Проблемою є визначення юридичної природи таких збоїв: чи є вони порушенням зобов'язання виконавцем, чи є наслідком незалежних обставин (форс-мажор). Оскільки ЦК України не містить норм про цифрову інфраструктуру як предмет підвищеного ризику, виникають труднощі у кваліфікації таких збоїв [13].

Міжнародні стандарти кіберстійкості (зокрема ISO/IEC 27001:2022) підкреслюють необхідність мінімізації ризиків технічної недоступності сервісів [22], однак національне законодавство прямо не встановлює вимоги до надійності онлайн-платформ.

Особливості укладення та виконання договорів онлайн-тренувань потребують фіксації доказів у цифровій формі: логів системи, історії платежів, даних про авторизацію, відеозаписів занять, електронного листування чи повідомлень у месенджерах. Закон України «Про електронну комерцію» вимагає забезпечення можливості збереження електронних документів та повідомлень [7], однак практичне застосування цієї норми вказує на брак єдиних стандартів фіксації автентичності та цілісності цифрових доказів [8].

Проблематичною є також судова оцінка електронних доказів: суди не завжди можуть підтвердити походження цифрового файлу; відсутність метаданих ставить під сумнів цілісність доказу; платформи не зобов'язані зберігати журнали логів тривалий час. Європейський підхід (Керівництво Ради Європи з електронних доказів) пропонує чіткі правила збереження цифрових даних [19], однак в Україні такі стандарти ще не імplementовані.

Онлайн-тренування передбачають обробку персональних даних, включно з відеозаписами, антропометричними характеристиками, повідомленнями приватного характеру. Такі дані часто належать до категорії чутливих, що підвищує вимоги до їх захисту. Закон України «Про захист персональних даних» та GDPR вимагають: чіткої та однозначної згоди суб'єкта; мінімізації обсягу оброблюваних даних; технічної безпеки та контролю доступу; заборони передачі третім особам без правових підстав [9; 28].

Ризики у сфері онлайн-тренувань включають: можливість витоку відеозаписів; зберігання даних на закордонних серверах без належних гарантій; використання інформації платформою всупереч договору; несанкціонований запис або поширення тренувальних матеріалів клієнтом чи іншими користувачами.



У цифровому середовищі відповідальність за порушення умов договору ускладнюється тим, що у наданні послуги беруть участь кілька суб'єктів: виконавець (тренер), цифрова платформа, платіжний провайдер, хмарний сервіс, провайдер відеозв'язку. Виникають проблеми: складність визначення виконавця у правовому сенсі; розмежування відповідальності між платформою та тренером; визначення збитків при технічному збої або недоступності сервісу; відсутність у ЦК України спеціальних правил відповідальності за цифровий контент і цифрові послуги.

Директива (ЄС) 2019/770 запроваджує модель відповідальності за «невідповідність цифрового контенту» [16], однак національне законодавство ще не адаптовано до таких стандартів.

Міжнародні стандарти й регіональні акти регулювання електронних договорів та онлайн-послуг демонструють декілька ключових підходів. UNCITRAL Model Law on Electronic Commerce (1996): встановлює принцип функціональної еквівалентності електронного правочину паперовому: «інформації не повинно відмовлятися в юридичній дії лише тому, що вона міститься у вигляді даного повідомлення» (Art. 5) та «вимога письмової форми задовольняється, якщо повідомлення доступне для подальшого посилання» (Art. 6) [34].

Підкреслюється технологічна нейтральність і невідмовність з правової дії електронним засобом. Директива (ЄС) 2019/770 «On certain aspects concerning contracts for the supply of digital content and digital services» встановлює правила для договорів надання цифрового контенту чи цифрових послуг, включно з оновленнями, відповідністю опису, засобами правового захисту при невідповідності та захистом персональних даних [16].

Європейський Союз також встановлює спеціальні правила для захисту споживачів при дистанційних договорах – наприклад, Директива 2011/83/EU про права споживачів визначає обов'язки надавача інформації, строки відмови та гарантії прозорості [18]. Порівнюючи: UNCITRAL задає загальні принципи (еквівалентність, технологічна нейтральність), тоді як акти ЄС – конкретні обов'язки для цифрових послуг, включно з гарантіями якості, оновленнями та правами споживачів.

В українському контексті Закон України «Про цифровий контент та цифрові послуги» фактично адаптує Директиву 2019/770 [10].

Таким чином, міжнародні підходи формують трирівневу нормативну структуру: • рівень принципів (UNCITRAL) [34]; • рівень конкретних правил для цифрового контенту/послуг (ЄС) [16–18]; • рівень національної імплементації (Україна) [10].

Узагальнення міжнародних підходів (UNCITRAL, Директива 2011/83/ЄС, Директива (ЄС) 2019/770, Регламент eIDAS, GDPR) дозволяє сформулювати комплекс пропозицій, спрямованих на підвищення правової визначеності онлайн-тренувальних послуг, зміцнення захисту прав споживачів та встановлення єдиних стандартів безпеки цифрових сервісів в Україні.

1. Необхідним є виокремлення договорів про онлайн-тренування як специфічного виду змішаних договорів, що поєднують надання послуг, доступ до цифрового контенту та елементи дистанційного навчання. Доцільно унормувати: визначення «онлайн-тренувальної послуги»; особливості предмета таких договорів; стандарт якості тренувальних програм; правила доступу до цифрових матеріалів, тривалість доступу та умови відновлення. Це відповідає підходу ЄС щодо виділення цифрових послуг як окремої категорії договорів [16].

2. Запровадити у Цивільному кодексі України спеціальну норму щодо укладення електронних договорів через платформи та мобільні застосунки; встановити обов'язковий мінімум інформації для споживача (аналог Директиви 2011/83/ЄС) [18]; урегулювати процедури акцепту у формах click-wrap та browse-wrap; зобов'язати платформи зберігати електронні журнали (логи) протягом визначеного строку. Це дозволить вирішити проблему доведення факту укладення договору та забезпечити прозорість для споживачів.

Висновки та пропозиції. Проведене дослідження дає змогу сформулювати комплексні висновки щодо особливостей цивільно-правового регулювання онлайн-тренувань та перспектив його вдосконалення з урахуванням міжнародних стандартів цифровізації.



По-перше, договори про надання онлайн-тренувальних послуг є змішаними за своєю правовою природою, поєднуючи елементи надання послуг, доступу до цифрового контенту та дистанційної взаємодії сторін. Їх укладення й виконання нерозривно пов'язані з технічними та організаційними характеристиками цифрового середовища, що вимагає адаптації договірних норм до специфіки платформи, цифрових сервісів та електронної комунікації.

По-друге, електронна та цифрова форма договору потребують чіткого визначення механізмів ідентифікації сторін, способів акцепту, порядку фіксації істотних умов та правил збереження електронних доказів. Проблеми автентичності, цілісності й допустимості цифрових доказів залишаються одними з ключових у правозастосовній практиці, що свідчить про необхідність оновлення процесуальних норм та розроблення стандартів електронного документообігу.

По-третє, специфіка онлайн-тренувань обумовлює підвищені ризики у сфері персональних даних, оскільки обробка відеоматеріалів, інформації про фізичний стан та персональних характеристик клієнтів потребує забезпечення високого рівня цифрової безпеки та відповідності вимогам національного й європейського законодавства про захист даних.

По-четверте, аналіз міжнародних підходів (ЮНСІТРАЛ, eIDAS, GDPR, Директива (ЄС) 2011/83, Директива (ЄС) 2019/770) свідчить про необхідність інтеграції принципів функціональної еквівалентності електронного договору, прозорості інформації для споживача, належної якості цифрової послуги й відповідальності за її невідповідність. Українське законодавство лише частково гармонізоване з цими стандартами й потребує подальшого розвитку.

По-п'яте, удосконалення цивільно-правового регулювання онлайн-тренувань має ґрунтуватися на: законодавчому закріпленні правового статусу онлайн-тренувальних послуг; деталізації правил укладення електронних договорів; запровадженні стандартів відповідальності за цифрові ризики; зміцненні гарантій обробки персональних даних; формуванні вимог до платформ-посередників; стандартизації цифрових доказів; розробленні типових договорів і галузевих рекомендацій.

Узагальнюючи, можна стверджувати, що правове регулювання онлайн-тренувань в Україні перебуває на етапі становлення та потребує комплексного вдосконалення з урахуванням міжнародного досвіду та зростаючих очікувань споживачів щодо прозорості, безпеки та передбачуваності цифрових сервісів. Реалізація запропонованих заходів сприятиме формуванню стабільного та захищеного цифрового середовища, підвищенню довіри користувачів та розвитку ринку онлайн-послуг.

Список використаних джерел:

1. Берч В. В. Правове регулювання електронної комерції: міжнародні та національні стандарти. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2, ч. 85. С. 11–16. DOI: <https://doi.org/10.24144/2307-3322.2024.85.2.1> (дата звернення: 21.11.2025).
2. Електронні правочини та інші нововведення Закону України «Про електронну комерцію». *KMP.UA*. 2015, 17 листоп. <https://kmp.ua/uk/analytics/infoletters/electronic-agreement-and-other-novelties-of-the-law-of-ukraine/> (дата звернення: 22.11.2025).
3. Кройтор В. А. Електронний договір. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 254–258. DOI: <https://doi.org/10.24144/2788-6018.2024.06.40> (дата звернення: 21.11.2025).
4. Логвінова М. В. Цивільна та сімейно-правова відповідальність батьків (осіб, які їх замінюють) за правопорушення, вчинені неповнолітніми : монографія. Івано-Франківськ, 2009. 206 с.
5. Правила надання послуг поштового зв'язку : постанова Каб. Міністрів України від 05 берез. 2009 р. № 270. *Законодавство України* : нормат.-прав. база / Верхов. Рада України. URL: <https://zakon.rada.gov.ua/laws/show/270-2009-п> (дата звернення: 22.11.2025).



6. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовт. 2017 р. № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400. Ред від 18.12.2024. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 22.11.2025).
7. Про електронну комерцію : Закон України від 03 верес. 2015 р. № 675-VIII. *Відомості Верховної Ради України*. 2015. № 45. Ст. 410. Ред. від 01.01.2024. URL: <https://zakon.rada.gov.ua/laws/show/675-19> (дата звернення: 22.11.2025).
8. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності : постанова Каб. Міністрів України від 01 серп. 2023 р. № 798. *Офіційний вісник України*. 2023. № 76. Ст. 4297.
9. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. Ред. від 14.06.2025. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 22.11.2025).
10. Про цифровий контент та цифрові послуги : Закон України від 10 квіт. 2023 р. № 2983-IX. *Відомості Верховної Ради України*. 2023. № 33. Ст. 337. URL: <https://zakon.rada.gov.ua/laws/show/3321-20> (дата звернення: 22.11.2025).
11. Цивільне право України. Частина загальна : підруч. / за ред. І. В. Спасибо-Фатєєвої. Харків : ЕКУС, 2024. 568 с.
12. Цивільне право України. Частина особлива : підруч. / за ред. І. В. Спасибо-Фатєєвої. Харків : ЕКУС, 2025. 592 с.
13. Цивільний кодекс України : станом на 22 січ. 2025 р. : відповідає офіц. тексту. Харків : Право, 2025. 432 с.
14. Annual Report – Trust Services Security Incidents 2024 / European Union Agency for Cybersecurity (ENISA). 2025. 26 p. DOI: <https://doi.org/10.2824/2144753> (last accessed: 21.11.2025).
15. Consumer Conditions Scoreboard: 2025 Edition / European Commission. Brussels, 2025. 52 p. URL: https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/key-consumer-data_en (last accessed: 21.11.2025).
16. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dir/2019/770/oj> (last accessed: 22.11.2025).
17. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on electronic commerce (E-Commerce Directive). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dir/2000/31/oj> (last accessed: 22.11.2025).
18. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dir/2011/83/oj> (last accessed: 22.11.2025).
19. Electronic Evidence in Civil and Administrative Proceedings : Guidelines adopted by the Committee of Ministers of the Council of Europe on 30 January 2019 and explanatory memorandum. 2019. 31 p. URL: <https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5> (last accessed: 22.11.2025).
20. Fortin J. Children's Rights and the Developing Law. Cambridge : Cambridge University Press, 2009. 592 p.
21. Hagel J. The power of platforms : Part of the Business Trends series. *Deloitte Insights*. 2015. 16 Apr. URL: <https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/platform-strategy-new-level-business-trends.html> (last accessed: 21.11.2025).
22. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. Geneva : Intern. Organization for Standardization, 2022. 35 p.
23. ISO/IEC 27002:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Controls. Geneva : Intern. Organization for Standardization, 2022. 137 p.



24. ISO/IEC 27701:2019. Security Techniques – Privacy Information Management. Geneva : Intern. Organization for Standardization, 2019. 65 p.
25. Klymchuk O., Finko A. Ukrainian Digital Content and Digital Services Law: A Missing Piece in the Regulatory Puzzle. *Sayenko Kharenko*. 2023, 18 Oct. URL: <https://sk.ua/ukrainian-digital-content-and-digital-services-law-a-missing-piece-in-the-regulatory-puzzle-of-the-digital-sector/> (last accessed: 22.11.2025).
26. Reed C., Murray A. Electronic Signatures: Law and Regulation. Oxford : Hart Publishing, 2019. 280 p.
27. Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes / Eds.: R. Brownsword, K. Yeung. Oxford : Hart Publishing, 2008. 370 p.
28. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (last accessed: 22.11.2025).
29. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj> (last accessed: 22.11.2025).
30. 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) (Text with EEA relevance). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (last accessed: 22.11.2025).
31. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services (eIDAS). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> (last accessed: 22.11.2025).
32. Smedinghoff T. J. Electronic Contracting, Online Services and Digital Economy. New York : IP Law Books, 2020. 410 p.
33. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996. *United Nations Commission on International Trade Law*. URL: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (last accessed: 22.11.2025).
34. United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005). *United Nations Commission on International Trade Law*. URL: https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications (last accessed: 22.11.2025).
35. Walden I. Computer Crimes and Digital Evidence. Oxford : Oxford University Press, 2020. 512 p.

Дата першого надходження рукопису до видання: 26.11.2025

Дата прийнятого до друку рукопису після рецензування: 15.12.2025

Дата публікації: 31.12.2025

