

ЮРИДИЧНА СИЛА ЕЛЕКТРОННИХ КОНТРАКТІВ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ДЛЯ РОЗВИТКУ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА

Швидкий розвиток цифрових технологій та масове розповсюдження електронних сервісів призвели до значного підвищення ролі електронних правочинів у цивільно-правовому обігу: від електронної комерції і надання послуг до токенизації активів і виконання смарт-контрактів на розподілених реєстрах. Це породжує нагальну потребу в чіткій правовій регламентації статусу електронних контрактів, їхньої юридичної сили та умов визнання й виконання в національному праві.

Міжнародна практика і модельні документи створюють основу для уніфікації підходів до електронних правочинів. Зокрема, UNCITRAL ухвалила Model Law on Electronic Transferable Records (MLETR) [1], що демонструє міжнародну тенденцію визнання електронних еквівалентів передаваних документів та встановлення принципу функціональної еквівалентності електронних записів матеріальним носіям. Цей підхід має важливе значення для торгівлі та транскордонних операцій, де невизнання електронних записів створює значні бар'єри.

На рівні Європейського Союзу (що є орієнтиром для гармонізації національного права в контексті євроінтеграції) діє Regulation (EU) No 910/2014 (eIDAS) [2], яка встановила правові рамки для електронної ідентифікації, електронних підписів і довірчих послуг. У 2021–2023 рр. відбувалося активне просування ініціатив ЄС щодо перегляду/розширення правил (ініціативи з європейським цифровим посвідченням, обговорення eIDAS-revision), що додатково підсилювало вимогу адаптувати національні правові режими до єдиних стандартів аутентифікації й довіри для електронних транзакцій.

Одночасно в ЄС і на міжнародній арені зростає увага до регулювання нових технологій (смарт-контракти, блокчейн) у контексті правової визначеності: розробляються й обговорюються спеціальні ініціативи щодо криптоактивів (наприклад, робота над MiCA у 2020–2023 рр.), що показує прагнення законодавців поєднати інновації з захистом учасників ринку. Ці ініціативи підкреслюють, що без сучасного регулювання юридична сила електронних угод може залишатися сумнівною, особливо в питаннях доказування, ідентифікації сторін та виконання.

Для України питання юридичного визнання електронних контрактів є практично значущим: невизначеність у законодавчому регулюванні статусу смарт-контрактів, правил доказування при застосуванні електронних доказів та транскордонного визнання електронних записів створюють ризики для бізнесу, перешкоджають інноваційним моделям роботи і можуть гальмувати інвестиційні ініціативи. Це робить дослідження проблем і перспектив

правового регулювання електронних контрактів нагальним для вдосконалення національної правової системи та її гармонізації з міжнародними стандартами.

Отож, розпочнемо наш аналіз із питання правового статусу електронних підписів різних рівнів (КЕП, УЕП, удосконалений підпис), що має значний вплив на встановлення належного способу підтвердження волевиявлення сторін. В даній сфері суспільних відносин правове регулювання здійснюється завдяки Закону України «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 року в редакції Закону від 01.12.2022 року. Саме даним законом була здійснена спроба вирішити проблему встановлення чіткої ієрархії та критеріїв юридичної сили для КЕП, УЕП та інших засобів електронної ідентифікації, проте вирішена вона лише частково. Йдеться про те, що Закон визначає рівні довіри до засобів електронної ідентифікації — високий, середній і низький: низький рівень довіри відповідає простому електронному підпису; середній — удосконалений електронний підпис (УЕП); високий — кваліфікований електронний підпис (КЕП) або печатка. Закон також дає визначення КЕП: «удосконалений електронний підпис, який створюється за допомогою засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа» [3]. Для УЕП є окреме визначення: УЕП “що базується на кваліфікованому сертифікаті відкритого ключа” — але при цьому, як зазначають, “не містить відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису”. Також у Законі є й конкретні вимоги до УЕП (стаття 17-1) — наприклад, про автентичність, цілісність, зв’язок з підписувачем.

Але є моменти, які залишаються проблемними або не зовсім “ієрархічними” з точки зору юридичної сили:

- Хоч рівні довіри встановлені, закон не чітко формалізує, що саме означає “юридична сила” кожного рівня — наприклад, чи будь-який УЕП автоматично прирівнюється до КЕП з точки зору дозвільних правочинів чи судового доказування;
- Закон не дає окремий статус “смарт-контрактам” — УЕП та КЕП регулюються, але питання, як електронний підпис взаємодіє з автоматизованими механізмами виконання (наприклад, у смарт-контрактах), прямо до цього закону не віднесено;
- Частина реалізації “рівнів ідентифікації” покладається на схеми електронної ідентифікації, стандарти та технічні регламенти (які затверджуються постановами КМУ), що робить “ієрархію” не лише законодавчою, а й технічною — і це може призводити до розбіжностей на практиці.

Тобто, Закон у редакції від 01.12.2022 дійсно передбачає ієрархію електронних підписів через рівні довіри та дає визначення КЕП і УЕП. Проте він не повністю вирішує всі питання, пов’язані з “юридичною силою” різних підписів у всіх контекстах (наприклад, довірою в контракті, електронних угодах чи смарт-контрактах), і ці аспекти потребують подальшої законодавчої та нормативної доопрацювання.

Також проблемним видається відсутність комплексного законодавчого підходу до електронних правочинів, оскільки регулювання розпорошене між

цивільним, господарським, процесуальним, податковим та спеціальним законодавством. Вирішенням було б звичайно прийняття комплексного акта (або пакету актів) щодо електронних правочинів, який би системно врегулював форму, порядок укладення, виконання, зберігання та оскарження електронних договорів. Проект Закону № 6447 від 17.12.2021 року «Про внесення змін до Цивільного кодексу України, спрямованих на розширення кола об'єктів цивільних прав», який коротко називають «Про цифрові речі» покликаний вирішити частково питання статусу “електронних правочинів”, але на жаль він не повністю покриває форму, порядок укладення, виконання, зберігання та оскарження електронних договорів. Ну і чи однотайними будуть депутати при його голосуванні також складно спрогнозувати, тому наразі констатуємо відсутність комплексного підходу до визнання смарт-контрактів, проте намагання вирішити означену проблему в рамках правового поля присутні.

Також наявними є проблеми доказування у суді електронних правочинів, пов'язані з відсутністю уніфікованих стандартів автентифікації, підтвердження цілісності та збереження електронних даних. Запровадження національних стандартів електронних доказів було б логічним вирішенням означеної проблеми, включаючи вимоги до автентичності, хешування, електронних журналів подій та цифрових слідів. Безумовно в Україні є національні стандарти та настанови, які регламентують окремі аспекти цифрових (електронних) доказів — ідентифікацію, збирання, здобуття, збереження та питання криптографічного захисту (хешування, алгоритми тощо). Однак ці стандарти не становлять єдиного вичерпного кодексу щодо всіх технічних вимог (журнали подій, форматів хешів, довготривалої архівації, універсального ланцюга зберігання тощо) — багато моментів залишаються на рівні методик, експертної практики та процесуального оцінювання судами.

У питанні транскордонного визнання електронних контрактів і підписів, що впливає на діяльність резидентів у міжнародному цифровому середовищі та уповільнює інтеграцію до європейського ринку, слід зосередитись на гармонізації нашого законодавства з міжнародними моделями, зокрема з eIDAS та актами UNCITRAL. Національне законодавство потребує комплексного оновлення, спрямованого на: запровадження сумісних із eIDAS категорій електронних підписів і довірчих послуг; узгодження принципів електронної комерції та електронних доказів з підходами UNCITRAL; створення механізмів автоматичного або спрощеного визнання іноземних електронних ідентифікаторів та підписів; забезпечення стабільного правового середовища для міжнародного цифрового бізнесу. І що важливо, навіть якщо Україна гармонізує своє законодавство до означених вимог, Європейський Союз надто обережно відноситься до визнання схем ідентифікації. Автоматично всі вони визнаватимуться за умови повної гармонізації лише через пару років.

Відсутність єдиного стандарту збереження електронних документів також ускладнює їх довгострокову юридичну придатність. У цьому відношенні слід було б запровадити національні вимоги до довгострокового архівування електронних документів із забезпеченням їх юридичної придатності та можливістю перевірки через десятиліття.

В ЄС є чіткий набір технічних профілів і норм, а також міжнародні/європейські добрі практики (ISO 16363 [4]) для того, щоб забезпечити довгострокову юридичну придатність електронних документів. Попри те, що це не один документ, все ж вказані документи об'єднані єдиною системою і в змозі виконати завдання по встановленні єдиних вимог до довгострокового архівування електронних документів. Україні слід вимагати сертифікацію/аудит сховищ за ISO 16363 або еквівалентною схемою для репозиторіїв, які надають архівні послуги з юридичною гарантією, а також визначити мінімальні технічні параметри (алгоритми хешування, політики зберігання ключів, часові мітки, вимоги до журналів подій) і вимагати їх дотримання в договорах/нормативах.

Отож, проведений аналіз свідчить, що питання юридичної сили електронних контрактів в Україні залишається комплексною проблемою, яка охоплює як технологічні, так і суто правові аспекти. Попри значні кроки вперед — оновлення Закону України «Про електронну ідентифікацію та електронні довірчі послуги», розвиток електронних сервісів, активізацію законодавчої роботи у сфері цифрових активів та електронних правочинів — національна система ще не наблизилася до рівня цілісності, що характерний для міжнародних та європейських стандартів.

Насамперед неврегульованими залишаються ключові питання:

- повна й однозначна ієрархія електронних підписів та межі їх юридичної сили;
- визначення статусу смарт-контрактів і інтеграція автоматизованих механізмів виконання у правове поле;
- системне регулювання електронних правочинів, включно з укладенням, виконанням, доказуванням та оскарженням;
- стандарти цифрових доказів, технічні вимоги до їх цілісності й довгострокового збереження;
- транскордонне визнання електронних підписів, ідентифікаторів та електронних записів.

У цьому контексті Україна потребує не точкових змін, а комплексної цифрової кодифікації, що має включати: гармонізацію з eIDAS та актами UNCITRAL, ухвалення технологічно нейтрального та узгодженого підходу до електронних договорів, створення єдиного стандарту електронних доказів, а також запровадження вимог до довготривалого архівування документів на основі міжнародних норм (зокрема ISO 16363).

Забезпечення правової визначеності в сфері електронних правочинів є не лише юридичною вимогою, але й передумовою для інноваційного розвитку, залучення інвестицій, зміцнення конкурентоспроможності українського бізнесу на глобальному ринку та інтеграції до цифрового простору ЄС. Від того, наскільки послідовно та системно Україна оновить своє законодавство, залежить можливість створити надійне й передбачуване середовище, в якому електронні контракти стануть не винятком, а повноцінним і гарантовано захищеним інструментом цивільного обігу.

Список використаних джерел:

1. UNCITRAL Model Law on Electronic Transferable Records (2017). [UNCITRAL Model Law on Electronic Transferable Records \(2017\) | United Nations Commission On International Trade Law](#)
2. Regulation (EU) No 910/2014 (eIDAS). [Regulation \(EU\) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC](#).
3. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
4. INTERNATIONAL STANDARD ISO 16363. Space data and information transfer systems — Audit and certification of trustworthy digital repositories. <https://cdn.standards.iteh.ai/samples/56510/bd62d68340e24e66a43571cadb1ff91c/ISO-16363-2012.pdf>