

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

**ІТ-ПРАВО
ПІД ЧАС ГІБРИДНОЇ ВІЙНИ:
ВІД ПОШУКУ ПАРАДИГМИ
ДО ПРАГМАТИЧНИХ РІШЕНЬ**

Колективна монографія

*За редакцією
Є. Харитонова, О. Харитонової, І. Давидової*

Одеса
Фенікс
2025

*Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)*

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

I-87 **ІТ-право під час гібридної війни: від пошуку парадигми до практичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонов, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ЗМІСТ

Авторський колектив	5
Розділ 1. Прагматична (соціологічна) школа «ІТ-права» – відповідь цивілістики на виклики інформаційного суспільства (Євген Харитонов, Олена Харитонova, Ірина Давидова)	7
Розділ 2. Концепт ІТ-права (Євген Харитонов, Олена Харитонova)	30
Розділ 3. Гібридна інформаційна війна та інформаційні технології (Євген Харитонов, Олена Харитонova)	65
Розділ 4. ШІ як бінарна категорія ІТ (Євген Харитонов, Олена Харитонova)	93
Розділ 5. Симулякр, гібридна (інформаційна) війна і потенціал ІТ (Євген Харитонов, Олена Харитонova)	119
Розділ 6. Інформаційне середовище як стратегічний ресурс у гібридних конфліктах (Оксана Калітенко)	143
Розділ 7. Правові рамки для цифрових активів: перспективи цифрової власності (Катерина Некіт)	175
Розділ 8. Захист немайнових прав у медіапросторі в період гібридної війни (Алла Кирилюк, Лариса Галупова)	203
Розділ 9. ІТ-правочини в умовах гібридної війни (Ірина Давидова)	250
Розділ 10. Порушення прав інтелектуальної власності в мережі інтернет під час гібридної агресії в умовах воєнного стану (Наталія Бааджи)	279
Розділ 11. Кіберзагрози у гібридній кібервійні: дія і протидія (Євген Харитонов, Олена Харитонova)	323
Розділ 12. Етико-юридичні аспекти використання штучного інтелекту в мережі інтернет в умовах гібридної війни (Олександр Омельчук)	351
Розділ 13. Застосування систем автоматизованого прийняття рішень під час збройного конфлікту (Віра Токарева)	378

Розділ 14. Гібридна війна і кіберзброя (Євген Харитонов, Олена Харитонova)	388
Розділ 15. Вербування неповнолітніх через соцмережі та месенджери в умовах гібридної війни: загрози, механізми та заходи запобігання (Вікторія Рябченко)	420
Розділ 16. Правове регулювання діяльності стартапів в умовах гібридної війни: виклики, можливості та перспективи (Дмитро Розумейко)	435
Розділ 17. Е-кредитування у період воєнного стану (Олена Берназ-Лукавецька)	453
Розділ 18. Цивільно-правова відповідальність за шкоду, завдану кібератаками (Богдан Фасій)	483
Розділ 19. Сімейні правовідносини в сфері інформаційних технологій в умовах гібридної війни (Оксана Сафончик)	514
Розділ 20. Забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні (Крістіна Дрогозюк)	545
Розділ 21. Кіберспортивна дипломатія: перспективи для України (Максим Ткалич, Юлія Толмачевська)	557
Список основних праць представників школи	565

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонova Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561), кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031), аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492), аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 9

ІТ-ПРАВОЧИНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

DOI

*Ірина Давидова**докторка юридичних наук, професорка*

Головною підставою виникнення цивільних правовідносин є правочин – один з найбільш поширених юридичних фактів сфери приватного права. Дослідження категорії «правочин» становить інтерес для багатьох науковців, практиків, здобувачів освіти. Разом з тим, в даному випадку важливим вважаємо послідовність та комплексність такого вивчення, аналіз факторів «сьогодення» (відповідно до часу проведеного дослідження) та формування в результаті такого дослідження уточнених теоретичних положень та практичних рекомендацій.

На даний час послідовність такого дослідження мною становить понад п'ятнадцять років, однак в даному розділі будуть підсумовані результати основних досліджень (на опубліковані дослідження будуть зроблені відповідні посилання), які стосуються розвитку категорії правочину в умовах розвитку інформаційного суспільства, в умовах дії екстраординарних правових режимів, а також в умовах ведення гібридної війни. Для зручності виділимо певні підрозділи.

«Традиційні» правочини¹

Згідно з частиною 1 ст. 202 ЦК України правочином є дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків.

Як правова категорія, правочини характеризуються сукупністю ознак, що дають можливість відмежовувати їх від інших юридичних

¹ Харитонов Є. О., Давидова І. В. Особливості підстав виникнення цивільних правовідносин у ІТ-сфері. *ІТ-право: поняття та сутність*: моногр. За ред. О. І. Харитонові, Є. О. Харитонова. Одеса: Фенікс, 2017. С. 170-184.

фактів. Це те, що правочин: 1) завжди є вольовим актом; 2) є дією, спеціально спрямованою на досягнення певного правового результату; 3) є дією суб'єктів цивільного (приватного) права; 4) завжди правомірною дією. Названі ознаки є загальними для усіх правочинів, а тому стосуються і правочинів, які укладаються в ІТ-сфері.

Варто згадати також, що в ІТ-сфері набули поширення дво- та багатосторонні правочини (договори). Зокрема, це ІТ-договори надання послуг програмного забезпечення або його розробки; ІТ-договори роботи із ФОП або програмістами; договори про юридичний супровід фрі-лансерів; договори про юридичний аудит ІТ-компаній; договори купівлі-продажу сайту, домену, бренду тощо; будь-які договори, укладені за участі інтернет-магазинів; договори про правове забезпечення діяльності інтернет-магазинів; концесійні договори; ліцензійні угоди; договори про сумісну діяльність у сфері ІТ-відносин; договори, об'єктом яких є права інтелектуальної власності.

Усі згадані договори мають відповідати загальним цивільно-правовим вимогам, що висуваються чинним законодавством до договорів, що зумовлене універсальністю категорії «договір» і придатністю її для використання у різноманітних сферах людського буття, в тому числі і в ІТ-сфері.

Разом із тим, між «ІТ-правом» і правочинами (договорами) існує своєрідний «зворотний зв'язок», що проявляється у коригуванні за допомогою його специфічних засобів «класичних» вимог, ознак, правил, які стосуються розуміння сутності, порядку укладення угод, їхньої форми тощо.

Це пов'язано з тим, що розвиток ІТ дозволяє створювати нові технологічні рішення та інструменти, які спрощують наше життя: як у виконанні простих буденних задач, так і у проведенні надзвичайно складних обчислень, моделювань та ін. Удосконалюються і елементарні процеси у здійсненні базових правовідносин, зокрема й у сфері ідентифікації.

Розглянемо це твердження спочатку на прикладі динаміки оформлення правочинів.

ЦК України (частини 1-3 ст. 207) визначає умови, за яких правочин може вважатися вчиненим в письмовій формі, а саме: якщо його зміст зафіксований в одному або кількох документах, у листах, телеграмах, якими обмінялися сторони; якщо воля сторін виражена за

допомогою телетайпного, електронного або іншого технічного засобу зв'язку; якщо він підписаний його стороною (сторонами). Правочин, який вчиняє юридична особа, підписується особами, уповноваженими на це її установчими документами, довіреністю, законом або іншими актами цивільного законодавства, та скріплюється печаткою. Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або іншого аналога власноручного підпису допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.

Отже, положення чинного законодавства даю можливість говорити про те, що використання ідентифікації, як інструменту встановлення особи, залишається необхідним при здійсненні відповідних правовідносин в електронній площині. Тому існує практична необхідність існування дієвої системи, яка б чітко надавала дозвіл на вчинення певних дій, отримання інформації саме тій особі, яка має право на отримання такої інформації, або вчинення відповідних правочинів. В даному випадку неможливо обійтися без електронних засобів ідентифікації, які мають прив'язку до особи (яку треба ідентифікувати за абсолютно різними характеристиками).

Однак, не достатньо розробити та застосовувати на практиці такі електронні засоби ідентифікації, має також існувати правове закріплення їх функціонування та правовий захист, яке сьогодні в українському законодавстві не є досконалим та потребують доопрацювання та оновлення. Ці питання є особливо актуальними, зважаючи на новизну у технічному застосуванні та необхідність врегулювання процесів встановлення особи, адже це найголовніша стадія здійснення будь-якому правочину.

Електронні правочини¹

За останні роки електронні правочини досить міцно укріпилися в нашому житті та набули особливого значення. Якщо спочатку це

¹ ІТ-право: практичний посібник. К.: Норма права, 2025. С. 132-138.

було спричинено розвитком технологій, як таких, та практичним їх застосуванням, то з часом додалися обмеження внаслідок запобігання розповсюдження короно вірусної хвороби, а тепер і введення воєнного стану та ведення на певних територіях нашої країни активних бойових дій.

Законодавець розрізняє поняття електронного правочину та електронного договору в Законі України «Про електронну комерцію». Зокрема, під електронним договором розуміється домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків і оформлена в електронній формі, а під електронним правочином – дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків, здійснена з використанням інформаційно-телекомунікаційних систем. Також ЦК України (починаючи з вересня 2015 року) прирівнює електронну форму вчинення правочину до письмової.

Вже згадуваний Закон під електронною формою представлення інформації розуміє спосіб документування інформації, що означає створення, запис, передачу або збереження інформації у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних або інших засобів, здатних до відтворення, передачі чи зберігання інформації. Таке документування інформації повинно надавати змогу її відтворювати у візуальній формі, придатній для сприйняття людиною.

Не секрет, що укладення договорів он-лайн має такі переваги, як швидкість, оперативний обмін інформацією, зручність зберігання, оброблення, відправлення документів тощо. А сьогодні можна й додати наявність такого важливого фактора, як безпека сторін, що є дуже важливим в умовах воєнного часу.

Договір як в «традиційному» розумінні, так і «електронний», мають відповідати чинному законодавству. Зокрема, пропозиція укласти договір (оферта) має містити істотні умови, передбачені законодавством для відповідного договору, і виражати намір особи, яка її зробила, вважати себе зобов'язаною у разі її прийняття.

Умови дійсності електронного договору можна поділити на традиційні та особливі. До традиційних можна віднести загальні умови дійсності, які передбачені законодавством (ст. 203 ЦК України) та додаткові, які передбачені сторонами і є обов'язковими для сторін, які

його підписали. До особливих умов можна віднести такі умови, які впливають із суті саме електронного договору, це, зокрема: електронна форма вчинення, використання відповідних засобів ідентифікації, електронна форма представлення інформації, спеціальні засоби безпеки тощо.

Отже, електронний договір, крім визначених ЦК України істотних умов для відповідного виду договору, може містити інформацію про: технологію (порядок) укладення договору; порядок створення та накладання електронних підписів сторонами договору; можливість та порядок внесення змін до умов договору; спосіб та порядок прийняття пропозиції укласти електронний договір (акцепту); порядок обміну електронними повідомленнями та інформацією між сторонами під час виконання ними своїх зобов'язань; технічні засоби ідентифікації сторони; порядок внесення змін до помилково відправленого прийняття пропозиції укласти електронний договір (акцепту); посилення на умови, що включаються до договору, шляхом перенаправлення (відсилання) до іншого електронного документа і порядок доступу до такого документа; спосіб зберігання та пред'явлення електронних документів, повідомлень, іншої інформації в електронній формі та умови доступу до них; умови виготовлення та отримання паперових копій електронних документів; можливість вибору мови, що використовується під час укладення та виконання договору тощо.

Електронний договір в межах чинного законодавства України розглядається як складова електронної комерції, а отже учасниками є суб'єкти електронної комерції, постачальники послуг проміжного характеру в інформаційній сфері, органи державної влади та органи місцевого самоврядування в частині виконання ними функцій держави або місцевого самоврядування. Законом визначено, що однією із сторін електронного договору обов'язково є юридична особа або фізична особа – підприємець (продавець (виконавець, постачальник) товарів, робіт, послуг). Слід зазначити, що на практиці велика кількість електронних договорів укладається саме між фізичними особами, які по суті відповідають спеціальному законодавству, однак не маючи статусу як мінімум ФОП, до них буде застосоване лиш базове законодавство, зокрема, ЦК України.

Відзначаючи специфіку електронних договорів, і враховуючи те, що важливим етапом укладення будь-якого договору є його підписан-

ня, зазначимо, що при укладенні договорів у цифровій (електронній) площині мова йде, насамперед, про ідентифікацію особи. Під такою ідентифікацією законодавець розуміє процедуру використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи, де ідентифікаційними даними особи є унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи.

Враховуючи те, що оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису (відповідно до Закону), законодавець закріпив рівні електронної ідентифікації, які можуть бути застосовані при вчиненні тих чи інших правочинів. Це, зокрема, високий, середній або низький рівні. Кожному з зазначених рівнів відповідають: кваліфікований, удосконалений та (просто) електронний підписи (КЕП, УЕП та ЕП відповідно).

Базовим законом в сфері ідентифікації осіб у електронній площині є Закон України «Про електронну комерцію», у ст. 12 якого зазначається, що «коли відповідно до акта цивільного законодавства або за домовленістю сторін електронний правочин має бути підписаний сторонами, моментом його підписання є використання: електронного підпису відповідно до вимог законів України «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги», за умови використання засобу електронного підпису усіма сторонами електронного правочину; електронного підпису одноразовим ідентифікатором, визначеним цим Законом; аналога власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів»¹.

У такому контексті виникає необхідність більш детально розглянути поняття криптографічного захисту інформації. У більшості

¹ Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. <https://zakon.rada.gov.ua/laws/show/675-19#Text>

країн, діяльність, яка пов'язана з криптографічним захистом інформації, підлягає правовому регулюванню. В Україні розробки в сфері криптографічного захисту інформації, також законодавчо закріплені. Зокрема, відповідно до ст. 7 Закону України «Про ліцензування видів господарської діяльності»¹ діяльність, пов'язана з наданням послуг в галузі криптографічного захисту інформації, ліцензується.

Визначення основних понять у сфері криптографічного захисту інформації міститься в Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України².

Отже, криптографічний захист – це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Разом з тим, безліч аспектів використання криптографії на законодавчому рівні в Україні залишаються неврегульованими. Зокрема, відсутні норми, які регламентують участь в діяльності, пов'язаній з криптографічним захистом інформації, фізичної особи без статусу суб'єкта господарювання. Також відкритим залишається питання про можливість примусового розкриття ключів шифрування користувачами на вимогу правоохоронних органів.

Особи, які прагнуть захистити власний особистий простір від несанкціонованого втручання шляхом розробки і застосування криптографічних алгоритмів і систем, в Україні мають можливість це зробити.

Технологія електронного підпису продовжує динамічно розвиватись. Наразі вже працюють сервіси, які допомагають встановити додаткові підстави довіри до особи, яка поставила на документі свій електронний підпис. В такому випадку, справжність електронного підпису перевіряється іншими сторонами правочину за раніше відомими ідентифікаторами, у відповідності до яких вони можуть ототожнити отриманий підпис з особою, яка вказана, за набором даних, доданих провайдером до електронного підпису.

¹ Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 № 222-VIII. URL: <https://zakon.rada.gov.ua/laws/show/222-19#Text>

² Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 р.№ 505/98. URL: <http://zakon3.rada.gov.ua/laws/show/505/98>

Така перевірка може відбуватись за номером телефону або електронною адресою, яка вказується при реєстрації в системі надавача послуги електронного підпису. Обов'язок провайдера – перевірити за допомогою спеціального посилання-активації профілю та одноразового sms-паролю справжність вказаних додаткових ідентифікаторів, а також їх належність особі, яка створила акаунт в системі.

Проте, відповідний ризик компрометації електронного підпису усе ж залишається, хоча і складно уявити одночасний несанкціонований доступ і до електронної пошти особи, і до мобільного телефону, попри те, що окремі сервіси реєструють користувачів у системах надання електронних підписів виключно на основі вказаної при реєстрації електронної пошти.¹

Ще одним введенням у дію електронним ідентифікатором в українському правовому полі на даний час є електронний підпис одноразовим ідентифікатором.² У Законі електронний підпис одноразовим ідентифікатором визначено як «дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору».³

Отже, виникає ситуація, коли особі, що прийняла оферту, на етапі підтвердження укладання відповідного електронного договору, надсилається одноразовий ідентифікатор, який згодом вводиться нею для підтвердження укладання такого договору. Такий спосіб здається цілком прийнятним, адже відбувається і перевірка контактного номеру, і встановлюється сам факт волевиявлення з приводу укладання такого договору.

Проте, в загальному ланцюгу забезпечення чинності договору, обов'язок ідентифікації покладається на самого акцептанта – замовника товарів чи послуг. Такий висновок можна зробити на основі частини 8 ст. 11 закону, в якій зазначається, що у разі, коли укладення електронного договору відбувається в інформаційно-телекомунікаційній системі суб'єкта електронної комерції, для прийняття пропо-

¹ Горкуша М. Встановлення довіри до електронного підпису в Україні. URL: <https://ilaw.net.ua/vstanovlennya-doviry-do-elektronnoho-pidpysu-v-ukrajini/>

² Горкуша М. Правові засади регулювання ідентифікаторів в Україні. URL: <https://ilaw.net.ua/pravovi-zasady-rehulyuvannya-identyfikatoriv-v-ukrajini/>

³ Про електронну комерцію: Закон України від 3 вересня 2015 р. № 675 VIII. *Офіційний вісник України*. 2015. № 78.

зиції укласти такий договір особа має ідентифікуватися в такій системі та надати відповідь про прийняття пропозиції. Іншими словами, йдеться про реєстрацію на сайті продавця із зазначенням відповідних ідентифікуючих даних, необхідних для укладання електронного договору, зокрема ім'я та прізвища, номера мобільного телефону (в контексті використання електронного підпису електронним ідентифікатором), e-mail та інших даних.

Однак магазин, все одно, не може перевірити надані параметри для ідентифікації. Адже повідомлення з одноразовим ідентифікатором буде надсилатись на вказаний особою мобільний телефон без встановлення особи. По суті, відбуватиметься лише підтвердження волевиявлення щодо особи із вказаними реєстраційними даними. Натомість, встановити дійсну належність цих даних зазначеній особі неможливо.

Крім того, в контексті пошуку використання більш безпечного варіанту слід згадати, що існує ще один ідентифікатор, більш універсальний за значенням і такий, що містить в собі той самий електронний цифровий підпис, – картка громадянина, або ж ID-картка, яка в українському законодавстві відображена як паспорт громадянина України у формі картки з безконтактним електронним носієм.

Важливим також є доповнення, зроблене в ЦК України (ч. 2 ст. 639 ЦК України) у грудні 2020 року, а саме: «Якщо сторони домовилися укласти договір за допомогою інформаційно-телекомунікаційних систем, він вважається укладеним у письмовій формі». Отже, в даному випадку ми бачимо, що мова йде про вчинення електронного правочину.

Аналізуючи судову практику можна зробити висновок, що електронна ідентифікація та підтвердження волі сторони договору укласти даний договір (взяти на себе передбачені даним договором права та обов'язки) шляхом використання електронного підпису, одноразових ідентифікаторів тощо є відповідним засобом ідентифікації особи, а тому на підставі використання електронних ідентифікаторів не можна говорити про визнання укладеного договору недійсним. В підтвердження цьому виступив і Верховний Суд, який розглянув у порядку письмового провадження справу про захист прав споживачів, визнання недійсним договору, захист персональних даних¹. Ана-

¹ Постанова Верховного Суду від 14 червня 2022 року у справі No 757/40395/20. URL: <https://reyestr.court.gov.ua/Review/104769406>

логічним є й висновок в Постанові Верховного Суду від 12 січня 2021 року¹.

Отже, можна погодитися з позицією Верховного Суду стосовно того, що будь-який вид договору, який укладається на підставі Цивільного або Господарського кодексів України, може мати електронну форму. Нині можна спостерігати значні можливості в сфері укладання договорів, підписування звітів, отримання державних послуг тощо он-лайн, доступ до яких відкривається шляхом електронної ідентифікації через електронний підпис.

Блокчейн²

Розвиток технологій у всьому світі з кожним днем набирає обертів. За останні роки, в умовах карантинів, можна було спостерігати не лише розширення застосування на практиці різного роду технологічних рішень, а й бачити все нові і нові відкриття. Важливою рушійною силою такого розвитку є, зокрема, бажання зекономити час, кошти (витрати), бути конкурентоздатним за умови великої конкуренції. Технологія блокчейн активно почала обговорюватися в більшості країн, зокрема, і в Україні, у 2017 році.

Під блокчейном необхідно розуміти розподілений публічний реєстр, заснований на сучасних криптографічних алгоритмах, що містить базу даних про всі раніше здійснені операції. Такий реєстр по своїй суті є децентралізованим. Дана система, за твердженням розробників, виключає крадіжку, шахрайство, порушення майнових прав тощо. Факти, що зберігаються в блокчейн не можуть бути загублені. Вони залишаються там назавжди. Крім того, блокчейн зберігає не лише кінцевий стан, а й усі попередні стани. Тому кожен може перевірити правильність кінцевого стану, перераховуючи факти від самого початку.

До переваг використання системи блокчейн відносимо: децентралізацію; доказовість кожної трансакції; прозорість; безпека; неможливість внесення змін у «підписаний» блок; обчислювальна логіка; економія часу; економія ресурсів.

¹ Постанова Верховного Суду від 12 січня 2021 року у справі № 524/5556/19. URL: <https://reyestr.court.gov.ua/Review/94102130>

² ІТ-право: практичний посібник. К.: Норма права, 2025. С. 139-145.

Разом з тим, поки ми ще не опанували повністю дані технології, а, отже, можемо говорити й про недоліки. Зокрема, це великі витрати електроенергії, проблеми з масштабністю, інерцією гравців ринку, необхідністю в деяких питаннях досягати консенсусу між великою кількістю учасників, відсутність законодавчої бази, навчання осіб-користувачів, придбання відповідного обладнання тощо (що в умовах воєнного часу ускладнює процес розвитку, чи хоча б втримання на тому рівні, що вже був досягнутий). Важливим також є питання «ментальної» та «моральної» готовності суспільства до активного використання у своєму житті таких сучасних технологій, адже хоч ми вже і звикли до Інтернету, де можна не лише скористатися інформаційними джерелами, але й проводити деякі власні операції, обмінюватися інформацією, використовувати соціальні мережі для спілкування, проходити навчання на відстані, проводити різного роду конференції, семінари, купувати та продавати товари тощо, здійснювати різного роду дії в рамках проєктів «електронного самоврядування» (що значно скорочує час та є вельми зручним), записатися на прийом до лікаря через електронну систему, подати позов до суду та отримати від суду документи в електронному вигляді та багато іншого, однак перевести абсолютно всі сфери свого життя в цифровий простір мабуть готовий не кожний.

Тому вважаємо, що для активного впровадження таких технологій як блокчейн необхідно не просто закріпити таку можливість, а сформувати єдину концепцію, яка б дала можливість поступово впроваджувати нові технологічні розробки, даючи можливість суспільству оцінити всі їх переваги, що згодом забезпечить гармонійний розвиток суспільства (зокрема, інформаційного), поєднає всі сфери життя в цілісний діючий механізм.

Отже, законодавець має забезпечити пріоритет «права над кодом», передбачити відповідні обмеження, яким має слідувати розробник або оператор коду. Адже, навряд чи можна характеризувати позитивно, наприклад, ситуацію коли код дозволятиме банку з огляду на прострочення по кредиту автоматично віддалено заглушити двигун вашого автомобіля, який опинився взимку на трасі, або блокування житла тощо.

Закріпити поняття блокчейну на законодавчому рівні вже мали місце. Зокрема, у жовтні 2017 року у Верховній Раді України був

зареєстрований проєкт Закону України «Про обіг криптовалют в Україні»¹, в якому під блокчейном розуміється децентралізований публічний реєстр усіх проведених криптовалютних транзакцій, які були проведені суб'єктом криптовалютних операцій, а користувачем системи блокчейн є будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка за допомогою власного та/або орендованого технічного обладнання підтримує працездатність системи блокчейн, здійснює проведення криптовалютних транзакцій та захисту системи блокчейн. Однак, даний документ на даний момент так і залишився проєктом, містить лиш деякі понятійні категорії та в основному описує криптовалюту, а не технологію блокчейн, правила її застосування на практиці та наслідки такого застосування.

Також маємо два визначення блокчейну в Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки², які по суті можна характеризувати як технічне та технологічне, відповідно: 1) програмно-комп'ютерний алгоритм децентралізованого публічного або приватного реєстру чи бази даних, функціонування якої забезпечується шляхом взаємодії через Інтернет однорангової мережі, або будь-яким іншим способом, що гарантує належний криптографічний захист усіх записів, транзакцій, проведених з використанням відповідної технології; 2) концепція, що може трансформувати державне управління в таких сферах, як реєстрація майнових прав, правосуддя, ідентифікація особи; як технологія довіри, блокчейн у державному секторі може використовуватися для електронних референдумів, петицій, голосування та інших сервісів електронного урядування; блокчейн забезпечує високоефективні механізми захисту цілісності та доступності інформації та дозволяє створювати повністю децентралізовані системи.

На даний момент можна констатувати, що найбільш активно розвивається застосування блокчейн-технології у сфері державних реєстрів. Однак, дана технологія може бути застосована у різних сферах нашого життя, зокрема, в банківській сфері, сфері страхування, освіти, держуправління, туризму, сферах розвитку штучного інтелекту,

¹ Про обіг криптовалют в Україні: проєкт Закону України № 7183 від 06.10.2017 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

² Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження Плану заходів щодо її реалізації: розпорядження КМУ від 17.01.2018 р URL: <http://zakon5.rada.gov.ua/laws/show/67-2018-p>

Інтернету речей, системи доменних імен, комп'ютерної безпеки, краудфандингових платформ, онлайн-ринків та ін.

Однак, задля реального та стрімкого розвитку даної технології необхідним є визначення її правового статусу, вирішення таких проблем правового характеру, як: відповідальність держави за функціонування системи («класичний» блокчейн не передбачає контролю взагалі, однак якщо мова йде про використання його державними органами, де може бути застосована інформація з обмеженим доступом тощо – має бути використаний власний «приватний» блокчейн і тут правові питання цілком можуть бути врегульовані нормами чинного законодавства щодо захисту інформації); стимул для підтримки функціонування системи користувачами; питання захищеності інформації (насамперед від втрати та спотворення).

Зокрема, користувачів точно будуть турбувати такі питання, як: можливість захисту авторських прав за допомогою блокчейна; використання інформації, яка охороняється законом, в блокчейн-продуктах (наприклад, персональні дані, державна, комерційна, банківська таємниця та ін.); наявність у сторін цивільно-правового договору право та дієздатності. Що також підтверджує необхідність законодавчого закріплення використання блокчейну.

Досить широке коло можливостей, які надає використання блокчейну, останнім часом обговорюють в сфері удосконалення економічних процесів. Це, зокрема, його впровадження в облікову систему, використання на фінансовому ринку, бухгалтерського обліку та аудиту, в сфері туризму, називають «новітнім фінансовим інститутом».

Можливим та достатньо надійним є перспектива використання блокчейн-технології для документування доказів воєнних злочинів рф в Україні. Таке фіксування надасть можливість в майбутньому використовувати дані про злочини в міжнародних судових процесах. А враховуючи те, що технологія блокчейн не дає можливість підробити чи змінити інформацію, яка там вже розміщена та визнається у всьому цивілізованому світі як надійна, можна сподіватися що зафіксовані докази будуть прийняти судами до уваги при винесенні рішень щодо притягнення до справедливих покарання військових злочинців.

Смарт-контракти¹

Аналіз впливу розвитку інформаційних технологій на категорію правочину свідчить про позитивні зрушення в сторону спрощення укладення правочинів. Спочатку з'явилася можливість вчинити традиційний правочин в електронній формі, яка передбачає фіксацію умов правочину не на папері, а за допомогою різноманітних електронних документів, ознайомлення з якими обов'язково має супроводжуватися використанням спеціального обладнання. Сьогодні на порядку денному – поява нового різновиду правочинів – смарт-контракту, виникнення якого пов'язують із появою криптовалют та технології блокчейн.

Смарт-контракт може існувати лише в цифровій мережі. Всі дані щодо згоди повинні знаходитися в блокчейні та мати однокористувачу правову цінність для сторін, які домовилися про вчинення правочину. Смарт-контракт також виступає посередником між сторонами, він не перераховує кошти на рахунок продавця до того часу, поки не будуть виконані певна частина, або всі дії щодо виконання смарт-контракту сторонами. Смарт-контракти дозволяють обмінюватися грошима, власністю, акціями або іншими активами у більш зручному режимі, аніж при укладенні традиційних договорів. Також, на відміну від традиційних правочинів, смарт-контракти, крім зберігання інформації про зобов'язання сторін і штрафи за їхнє порушення, самі (автоматично) забезпечують виконання всіх умов правочину. Весь цей час документ зберігається і дублюється в децентралізованому реєстрі, що забезпечує його надійність і не дозволяє жодній зі сторін змінювати умови правочину.

Практичне застосування смарт-контрактів можливе у багатьох сферах, зокрема, у фінансовій сфері при кредитуванні, бухгалтерському обліку тощо (наприклад, для оцінки ризиків та аудиту в режимі реального часу); у сфері розвитку міста (розумний автомобіль, розумний будинок тощо); в юриспруденції (наприклад, при винесенні рішень суду, за умови використання технології «комп'ютерного судді», яка була створена науковцями Університетського коледжу Лондона та Університету Шеффілда). Однак, поки йдеться про аналіз даних та визначення можливого варіанта за принципом вірогідності,

¹ ІТ-право: практичний посібник. К.: Норма права, 2025. С. 146-150.

на законодавчому рівні використовувати в повній мірі смарт-контракти як повноцінну альтернативу традиційним договорам немає підстав. Досить великі надії у впровадженні смарт-контрактів мають представники бізнесу, які вбачають в них перспективи підтримання та розвитку своїх напрямів, отриманні значних прибутків завдяки використанню передових технологій та програм, конкурентоспроможності на міжнародних ринках тощо.

Використання такого роду технологій (як блокчейн) та програм (як смарт-контракт) в зазначених сферах мають свої позитивні та негативні риси. Однак можна зазначити, що глобалізація сама по собі передбачає уніфікацію всіх процесів незалежно від країни, фактично «стираються» всі кордони, мова йде про суспільство як цілісну систему, яка живе за єдиними принципами, правилами, нормами, традиціями та законодавством, яке відповідає цим загальноприйнятим нормам.

Аналіз практичного застосування смарт-контрактів показав, що вони є доволі ефективними та дійсно мають багато позитивних рис, але поки це окремі великі угоди (як, наприклад, міжнародні операції з поставки товарів, міжбанківські комерційні договори тощо), які не є масовими та не мають єдиного технологічного «шаблону».

Цікаво, що вперше концепцію смарт-контракту було викладено ще у 1994 році, однак тоді мова йшла про електронний протокол передачі інформації. Наступним «кроком розвитку» став 2010й рік, а саме набуття популярності криптовалют. Такі контракти могли бути записані у вигляді коду, збережені і продубльовані у системі, а їх виконання забезпечить мережа комп'ютерів, керуюча блокчейном. Тобто, під смарт-контрактом вже розуміли контракт на даних розподіленого реєстру блокчейн.

Головною метою розробників смарт-контракту було – відмовитися від централізації, тобто щоб всі системи взаємодіяли але не підпорядковувалися одній головній системі. В даному контексті важливим є визначення правового статусу такої програми як смарт-контракт, визнання її на законодавчому рівні як повноцінної альтернативи традиційній формі договору, фактично, вірівненню ситуації. В умовах рекодифікації цивільного законодавства важливим є передбачення таких правових конструкцій, які б враховували не лише сучасний ступінь розвитку технологій, а й передбачали подальший їх розви-

ток, були спроможні забезпечити правове регулювання новітніх ІТ рішень у сфері укладення договорів.

Аналіз іноземного законодавства на предмет регулювання питань щодо смарт-контрактів дає можливість стверджувати, що світ лиш придивляється до даних «нових можливостей» і не має єдиного підходу до законодавчого регулювання даних питань. Зокрема, нині юридичне визнання смарт-контрактів з фіксацією правових наслідків найбільше поширене в США, зокрема в таких штатах, як Арізона, Каліфорнія, Теннессі, Делавер, Вайомінг, Небраска, Іллінойс. Їх резиденти можуть використовувати цифрові автоматизовані смарт-контракти з юридичною підтримкою, навіть якщо вони не забезпечені класичними письмовими контрактами. В Європейському Союзі дане питання частково регулюється, зокрема, дії в договірних відносинах у комерційній та цивільній сферах можуть тлумачитися як розумні контракти. Однак, є й країни які лиш «придивляються» до смарт-контрактів, або ж чітко визначають їх «різновидом» традиційного контракту. Більшість науковців та практиків переконані, що всі поточні питання адаптації смарт-контрактів до законодавства будуть усунені, а сама технологія буде стрімко розвиватися, охоплюючи все нові сфери діяльності.

Все зазначене дає можливість стверджувати, що смарт-контракт є правовим договором, який має перспективу укріпитися в практичному використанні та, з часом, зайняти провідне місце в забезпеченні сфери договірного права.

Звичайно, для смарт-контракту необхідним є існування таких обов'язкових елементів, як: цифрова ідентифікація всіх цифрових сторін договору; використання приватного децентралізованого середовища, в яке і будуть записуватися смарт-контракти; конкретно описані умови виконання смарт-контракту, які учасники підтверджують одночасно. Важливим тут є й вільне волевиявлення сторін укласти даний контракт, однак саме щодо цього пункту є досить багато дискусій, адже сторони віддалено ідентифікуються і немає впевненості в тому, що відсутній примус, обман тощо. Також задля дійсності такого контракту та визнання його на рівні з традиційним договором необхідним є й дотримання всіх інших істотних умов, які є обов'язковими при вчиненні «звичайного» договору.

Також, як і в будь-якій сфері, не обходиться без «проблем». В контексті використання смарт-контрактів можна виділити два проблемних «напрямки»: технічний та правовий. До першого можна віднести проблеми, пов'язані з тим, що самі розробники та програмісти не завжди чітко уявляють характер функціонування смарт-системи. Зокрема, можуть виникати наступні проблеми: забезпечення конфіденційності; асекурація безпеки; масштабність; не вирішено питання про можливі об'єктивні причини неможливості виконання контракту у певний час.

До проблем правового характеру можна віднести наступне: втрачається значення поняття «зобов'язання», адже в смарт-контракті сторони виражають волю один раз, а саме в момент його укладення; існує припущення, що смарт-контракт не може бути порушений, отже не може мати місця ситуація, коли одна із сторін не виконує або неналежно виконує договір у випадку коли вважає, що в світлі обставин, що змінилися його невиконання вигідніше, ніж виконання. Таким чином, сторони не можуть зважаючи на нові обставини (навіть об'єктивні) відмовитися від виконання договору. Фактично, не можна говорити і про примушування до виконання зобов'язання в натурі; смарт-контракт не враховує можливість наявності таких вад при укладенні правочину, як наприклад, вади суб'єкта, вади волі тощо. Зазначені обставини мають бути враховані і не можуть ігноруватися, вони є підставою визнання правочину недійсним; смарт-контракти не передбачають можливості захисту слабкої сторони (наприклад, споживача); можливість використання смарт-контрактів у незаконних цілях або укладання контрактів, які порушують публічний порядок. При цьому не можна ігнорувати насторожене ставлення до криптовалют з боку низки державних органів у різних країнах; надмірна автономність смарт-контракту, що визнають і програмісти, стверджуючи, що функціонуванню цього виду контрактів не потрібна правова система, оскільки такі контракти можуть існувати і поза правом, як децентралізовані альтернативи цілісній правовій системі.

Наразі, чинний Закон України «Про електронну комерцію» визначає, що документування інформації повинно надавати змогу відтворювати її у візуальній формі, придатній для сприйняття людиною. Таке формулювання не відповідає концептуальному розумінню сутності смарт-контрактів як таких, а тому даний Закон не

може застосовуватися до регулювання такого типу договорів, як смарт-контракти.

Отже, враховуючи вже існуючу практику застосування таких технологій у світі можна зробити висновок про позитивні очікування від укладення договорів у вигляді смарт-контрактів, до яких зокрема, віднесено об'єднання всіх учасників договору в загальну мережу; доступність актуальної інформації про договір відразу всім її учасникам; виписування всіх документів в оригінальному вигляді всередині системи; неможливість підробки документів; відсутність потреби пересилки паперових версій документів на великі відстані; автоматична перевірка системою документів (або взагалі контроль за фактом відвантаження) і здійснення платежів. Таким чином, можна говорити про перспективність використання блокчейну, смарт-контракту і Інтернету речей у певному симбіозі. Нині ж можна говорити про можливість поєднання традиційного та нового формату, наприклад, укласти традиційний договір та передбачити його виконання за допомогою відповідної комп'ютерної програми. Це дозволить виконати вимоги чинного законодавства щодо умов укладення договору та отримати сторонам «вигоди» смарт-контрактів, зокрема, автоматичність виконання, безпеку, швидкість тощо.

Використання штучного інтелекту для укладення смарт-контрактів

Інтеграція штучного інтелекту в процес розробки, аналізу й автоматизації смарт-контрактів відкриває нові горизонти для підвищення ефективності, надійності та безпеки цифрових трансакцій.

Термін «смарт-контракт» розуміють як: по-перше, як програмний код, що автоматично виконується при дотриманні визначених умов (його функціонування забезпечується децентралізованою мережею блокчейну); по-друге, як цифрову угоду, яка автоматично виконує умови, закладені в її коді. Такі контракти функціонують у децентралізованих середовищах, зокрема на платформах Ethereum, Binance Smart Chain, Solana тощо. Вони є незмінними, прозорими та виконуються без посередників.

Під терміном «штучний інтелект» розуміють: по-перше, сукупність алгоритмів і методів, які дозволяють комп'ютерним системам імітувати людський інтелект, включаючи навчання, логіку, прогнозування та прийняття рішень; по-друге, галузь комп'ютерної науки, яка створює системи, здатні до самостійного навчання, прийняття рішень, розпізнавання мовлення, зображень та логічного мислення. У поєднанні з блокчейн-технологіями штучний інтелект виступає інструментом для аналізу великих обсягів даних, автоматизованої генерації коду та виявлення аномалій.

Аналізуючи питання використання штучного інтелекту для укладення смарт-контрактів, можна виділити певні етапи життєвого циклу смарт-контрактів та можливість (перспективність) застосування штучного інтелекту на кожному з виокремлених етапів. До етапів життєвого циклу смарт-контрактів віднесемо їх розробку, аналіз та верифікацію, автоматизацію укладення угод, а також виконання та моніторинг.

Отже, на етапі розробки смарт-контрактів штучний інтелект може автоматично генерувати код смарт-контракту на основі текстового опису умов угоди. Наприклад, використання великих мовних моделей, таких як GPT, дозволяє конвертувати юридичну мову в код на мовах Solidity або Vyper. Наприклад, юридична компанія Legalese розробила платформу, що дозволяє створювати смарт-контракти за допомогою інтерфейсу природної мови (користувач просто вводить умови договору, а система генерує валідний код для Ethereum).

На етапі аналізу і верифікації смарт-контрактів штучний інтелект здатен виявляти логічні помилки, вразливості та невідповідності в коді контракту. Використання методів машинного навчання дозволяє аналізувати великі обсяги даних із попередніх контрактів та прогнозувати ризики, виявити вразливості до їх розгортання в мережі. Інструменти на базі штучного інтелекту вивчають тисячі попередніх смарт-контрактів, ідентифікуючи небезпечні шаблони. Наприклад, інструмент MythX (партнер ConsenSys) використовує штучний інтелект для автоматизованого аудиту смарт-контрактів, він аналізує код Solidity, виявляє помилки безпеки та пропонує виправлення.

На етапі автоматизованого укладення угод системи на базі штучного інтелекту можуть автоматично знаходити найвигідніші умови для укладення угоди (наприклад, у сфері децентралізованих фі-

нансів), проводити переговори та адаптувати умови контракту під потреби сторін. Також штучний інтелект може виступати як інтелектуальний агент-посередник, який веде переговори між сторонами, формує оптимальні умови та укладає угоду. Такі агенти здатні оцінювати ринкові умови, враховувати юридичні обмеження і навіть використовувати блокчейн-орекли для отримання актуальної інформації. Наприклад, у децентралізованих фінансах платформа Kleros використовує штучний інтелект для вирішення спорів між сторонами смарт-контракту, залучаючи децентралізованих арбітрів.

Наостанок, на етапі виконання контрактів та проведення моніторингу інтелектуальні агенти можуть контролювати зовнішні дані (oracles), аналізувати їх та ініціювати виконання контракту при настанні обумовлених подій. Після активації смарт-контракту штучний інтелект може контролювати зовнішні джерела даних (наприклад, ціни з бірж, погодні умови, результати матчів) та запускати виконання контракту при настанні обумовлених умов. Наприклад, у сільськогосподарському страхуванні смарт-контракт може автоматично виплатити компенсацію фермеру у разі посухи, якщо погодний API повідомляє про відсутність дощів понад 30 днів (штучний інтелект використовується для валідації даних та фільтрації аномалій).

До переваг інтеграції штучного інтелекту в роботу із смарт-контрактами можна віднести: автоматизацію юридичних процесів і зменшення людського чинника; підвищення безпеки за рахунок виявлення вразливостей до моменту публікації контракту; оптимізацію вартості укладення угод; гнучкість та адаптивність контрактів до динамічних умов; зменшення витрат внаслідок відсутності потреби у посередниках (нотаріуси, юристи); прогнозування ризиків, адже штучний інтелект може проаналізувати історію контрагентів та виявити шахрайські дії; масштабованість; юридична прозорість, адже коди відкриті для перевірки, а історія виконання незмінна.

Окрім переваг варто виділити й певні виклики та обмеження, які існують на практиці. Зокрема, сюди варто віднести: юридичну невизначеність (смарт-контракти та штучний інтелект не завжди мають чітке правове регулювання); проблема інтерпретації (автоматизовані контракти не завжди враховують неоднозначність юридичної мови); проблеми етики та довіри до автономних рішень, що приймаються штучним інтелектом; технічна складність у забезпеченні пов-

ної прозорості та пояснюваності рішень штучного інтелекту; питання безпеки (попри аудит, існує ймовірність хакерських атак через помилки в логіці контракту або алгоритмах штучного інтелекту).

Враховуючи перспективність даного напрямку, у майбутньому варто очікувати появу повністю автономних систем, які зможуть вести переговори, укладати угоди, перевіряти дотримання умов і забезпечувати виконання контрактів без втручання людини. Особливий інтерес викликає застосування генеративного ШІ для автоматичної розробки «легальних цифрових агентів» у сфері Web3. В межах зазначеного вважаємо за необхідне роботу в таких напрямках: розробка інструментів для підвищення довіри до рішень системи; створення стандартів юридичної відповідності для смарт-контрактів у різних юрисдикціях; вдосконалення багатомовних моделей, які дозволять працювати з договорами у різних правових системах; інтеграція смарт-контрактів у системи цифрової ідентичності; розробка легальних агентів. Тобто штучного інтелекту, що може виступати в суді або арбітражі в якості сторони угоди.

Підводячи підсумок варто зазначити, що інтеграція штучного інтелекту в екосистему смарт-контрактів є логічним кроком на шляху до повної автоматизації юридичних і фінансових процесів у цифровому середовищі. Хоча існують певні бар'єри, потенціал цієї синергії обіцяє значне підвищення ефективності, безпеки та доступності правових механізмів у цифровій економіці.

Інтеграція штучного інтелекту в екосистему смарт-контрактів є потужним кроком до формування «розумної економіки», де угоди укладаються без конфліктів, з мінімальною участю людини. Водночас подальше поширення таких рішень потребує оновлення правового поля, удосконалення технологій безпеки та розвитку інфраструктури пояснюваних ШІ-систем.

Правочини в умовах ковіду та воєнного стану¹

Повномасштабний початок ведення війни країною-агресором проти нашої держави спонукав до необхідності швидкого реагуван-

¹ Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: моногр. За ред. Харитоновна Є. О., Харитонвої О. І., Некіт К. Г. 2023. С. 113-122.

ня представників влади, державних органів, населення з метою вирішення великої кількості питань, з якими раніше ми не стикалися (принаймні в такому масштабі).

Внаслідок введення воєнного стану на території України відбулося багато змін правового характеру, зокрема, ми спостерігаємо стрімке превалювання публічного інтересу над приватним, необхідність жити за «новими правилами» з різного роду обмеженнями, зокрема, інтересів приватних осіб. Однак маємо пам'ятати, що в правовій державі, якою є Україна, не можна допустити порушення законних прав та інтересів суб'єктів правовідносин, зокрема, суб'єктів цивільних правовідносин. В даному контексті інститут правочину відіграє важливу роль, адже щодня ми стикаємося з необхідністю вчинити той чи інший правочин, а воєнний стан (що є специфічним та новим для кожного з нас) іноді потребує ще більш швидкого реагування та прийняття рішення про вчинення правочину (як, наприклад, укладення договору дарування, складання заповіту, довіреності тощо).

Необхідно зазначити, що формування інформаційного суспільства, глобалізаційні та інтеграційні процеси відбуваються вже не перший рік, що зумовило необхідність удосконалення правового інструментарію торгового обігу, а відтак і перегляду низки відомих цивільно-правових категорій, комплексного оновлення цивільно-правових норм, закріплених в Цивільному кодексі, що отримало назву «рекодифікації». В межах такої рекодифікації було піднято питання про формування нової концепції «правочину», трансформації розуміння даного поняття.¹

Спочатку ми навчилися за допомогою використання інформаційних технологій готувати до укладення та здійснювати процес укладення правочинів, тобто вчиняти їх в електронній формі. З вересня 2015 року в спеціальному нормативно-правовому акті, а саме Законі України «Про електронну комерцію»² було закріплено такі поняття,

¹ Давидова І. В. Формування нової концепції правочину в умовах рекодифікації цивільного законодавства. *Рекодифікація цивільного законодавства в умовах євроінтеграційних процесів*: моногр. За ред. Є. О. Харитонов, О. І. Харитонові. Київ: Норма, 2020. С. 68–81; Харитонов Є. О., Давидова І. В. Договори та правочини у Книзі першій ЦК України: «рекодифікаційний» потенціал: *Оновлення Цивільного кодексу України: формування підходів*: колективна моногр; за ред. Довгерт А. С., Харитонova Є. О. Одеса: Гельветика, 2020. С. 77–91.

² Про електронну комерцію: Закон України від 03.09.2015 р. URL: <https://zakon.rada.gov.ua/laws/show/675-19>

як «електронна торгівля», «електронний правочин», «електронний договір» тощо. Це певною мірою вплинуло на умови та порядок вчинення правочинів, визначення їх сторін, наслідки невиконання тощо, однак, практично, не змінило саме розуміння їхньої сутності. Аналіз же сформульованих понять дав можливість зробити висновок про те, що законодавець має на увазі правочини у традиційному його розумінні, оскільки змінюється лише характер спілкування сторін, спрощення вимог до оформлення правочинів тощо. Разом з тим, на нашу думку, мова йде не просто про електронну форму правочину, а про формування нової категорії, яка є наслідком формування інформатизації суспільства.

Таке забезпечення можливості в межах закону вчиняти правочини в електронній формі, без укладення паперових договорів, присутності сторін при його укладенні тощо є лише «перехідним» етапом та дає підґрунтя (основу) для формування правочинів «нового типу» (так званих «розумних» контрактів, які частіше позначаються терміном «смарт-контракти»¹). Їх можна назвати «перспективними» правочинами, тобто такими, які можуть стати «звичайною справою» через 10-15 років.

Внаслідок поширення інформаційних технологій (зокрема, таких як блокчейн) та програм (таких як «смарт-контракт» тощо) та їхніх відчутних переваг ведеться мова не лише про удосконалення порядку укладення правочину, а про зміну самого розуміння його сутності. Тобто про існування нового типу правочинів, що формується в інформаційному суспільстві, до якого, на нашу думку, мають бути віднесені правочини, котрі сутнісно пов'язані з використанням інформаційних технологій. Із врахуванням цієї їх особливості вони можуть іменуватися «ІТ-правочини»².

Блокчейн, як інструмент реалізації різних важливих проєктів не лише в сфері бізнесу, але й державному регулюванні знаходиться на початку свого шляху. За твердженням розробників дана система виключає крадіжку, шахрайство, порушення майнових прав тощо. Факти, що зберігаються в блокчейн не можуть бути загублені.

¹ Терміни «смарт-контракт», «розумний контракт» є традиційними, однак тут мається на увазі будь-які правочини (як одно-, дво- та багатосторонні договори, які можуть вчинятися суботами цивільних правовідносин).

² Давидова І. В. Правочини та їх недійсність в інформаційному суспільстві: автореф. дис. ... д-ра юрид. наук: 12.00.03. Одеса, 2018. С. 17.

Що ж стосується «смарт-контрактів», то це контракт на даних розподіленого реєстру блокчейн, де основою його реалізації є програмування з використанням принципу «якщо..., то....», тобто умова прямо визначена в контракті.¹

Першим викликом, який суспільство намагалося подолати, стала коронавірусна хвороба. Це був виклик як для суспільства в цілому, так і для кожного окремо. Крім необхідності дотримуватися певних правил та обмежень, постраждала економіка багатьох країн світу, актуалізувалися питання співвідношення публічних та приватних інтересів, пріоритетність питань стосовно здоров'я, а не «роботи до виснаження», адже навіть «просто послаблений імунітет» міг спричинити, як наслідок, серйозне захворювання і навіть смерть.

Так, ст. 29 Закону України «Про захист населення від інфекційних хвороб», постановою Кабінету Міністрів України від 11 березня 2020 р. № 211 «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» з 12 березня 2020 р. до 22 травня 2020 р. було встановлено на всій території України карантин, який передбачав ряд обмежень та правил, які мають на меті запобігти поширенню даного захворювання. Зокрема, відповідно до Порядку проведення протиепідемічних заходів, пов'язаних із самоізоляцією осіб, який також затверджений 11 березня 2020 року, досить велика група людей підлягала самоізоляції, серед яких: особи, які мали контакт з пацієнтом з підтвердженим випадком COVID-19; особи, щодо яких є підозра на інфікування, або особи, які хворіють на COVID-19 в легкій формі та не потребують госпіталізації; особи, що дали згоду на самоізоляцію з використанням електронного сервісу «Дій вдома» Єдиного державного веб-порталу електронних послуг; особи, які досягли 60-річного віку (за деякими винятками). Також до цієї групи можна віднести і осіб, які не досягли 14 років, яким відповідно до аналізованої Постанови заборонено пересуватися без супроводу законних представників або повнолітніх родичів дитини. Отже, досить велика група осіб повинна була здійснювати покупки не виходячи з дому.

Виходом з ситуації тут стало більш активне використання можливостей інформаційних технологій при вчиненні правочинів, зокрема,

¹ Що таке Смарт-Контракт? URL: <http://ethereum.net.ua/discussion/34/scho-take-smart-kontrakt>

при купівлі товарів, де інтернет-магазини і служби доставки мали чи не найбільший попит. Крім того, звичайні крамниці, які не мали права працювати офлайн (наприклад, крамниці одягу, взуття тощо) і мали офіційний сайт «номінально», – перейшли в он-лайн простір та намагаються втримати своїх клієнтів.

Коронавірус, звичайно, завдав багато шкоди людству, однак частково «підготував» нас до необхідності працювати та комунікувати онлайн. Виходом з ситуації при укладенні правочинів стало активне використання можливостей інформаційних технологій, зокрема, при купівлі товарів, де інтернет-магазини і служби доставки мали чи не найбільший попит. Крім того, звичайні крамниці, які не мали права працювати офлайн (наприклад, крамниці одягу, взуття тощо) і мали офіційний сайт «номінально», – перейшли в онлайн простір і намагалися максимально втримати своїх клієнтів.

Таким чином, із запровадженням обмежувальних заходів ми спостерігали ситуацію, коли звичні для нас (традиційні) договори трансформуються за допомогою запровадження інформаційних технологій в електронні договори, смарт-контракти тощо, які можуть укладатися сторонами без особистого контакту, паперових копій договорів, особистих (власноручних) підписів тощо. Це свого роду нова фаза розвитку, момент, який має відбутися не лише в сфері технічного забезпечення можливостей такого укладення правочинів, але й в свідомості кожної особи.

Враховуючи те, що учасниками цивільних правовідносин є фізичні та юридичні особи, а також держава Україна, Автономна Республіка Крим, територіальні громади, іноземні держави та інші суб'єкти публічного права, всі вони можуть бути сторонами договорів, у будь-якому сполученні, зокрема: між фізичними особами; між фізичними та юридичними особами; між юридичними особами; між фізичними особами та публічними утвореннями тощо.

Зазначимо, що розвиток інформаційного суспільства та інформаційних технологій, який зробив популярним укладення договорів он-лайн, має такі переваги, як швидкість, оперативний обмін інформацією, зручність зберігання, оброблення, відправлення документів тощо. В умовах необхідності віддаленої роботи він набув особливої актуальності, адже вчинення договорів за допомогою інформаційних технологій є не просто актуальним, а життєво необхідним для

суспільства, особливо для осіб, що перебувають на самоізоляції (за умови, коли мова йде про пандемію) або ж взагалі в іншому регіоні чи іншій країні (за умови, якщо ми говоримо про воєнний стан), належать до групи ризику, не мають можливості самостійно здійснити покупки тощо. Крім цього, внаслідок обмежень необхідний товар (непродовольчого призначення, в який входить великий перелік нагально необхідних речей) може бути доступним лише в інтернет-магазині. Тому аналіз правової природи, сутності електронних договорів, смарт-контрактів, їх особливостей є дуже актуальним. Знов таки, не всі регіони нині можуть отримати бажаний товар, адже не всі поштові відділення працюють і не на всіх складах є відповідні товари. Також у контексті воєнного стану ми стали свідками того, що логістична проблема є набагато більшою та глибшою, аніж можна було собі уявити.

Як уже було зазначено вище, законодавець виділяє як традиційне поняття «договір», що закріплене в ЦК України, так і поняття «електронний договір». Оферта має містити істотні умови, передбачені законодавством для відповідного договору, і виражати намір особи, яка її зробила, вважати себе зобов'язаною у разі її прийняття. Важливими тут є як «традиційні» так і «особливі» умови дійсності відповідного договору.

В умовах введення воєнного стану та проведення активних бойових дій на території України вчинення електронного правочину, а також можливість його виконання або ж вчинення необхідних дій для уточнення умов тощо має важливе практичне значення, а іноді це єдина можливість захистити права та інтереси осіб в умовах що склалися. Саме практична значущість та необхідність вчинення відповідних дій у «віддаленому» форматі є забезпеченням можливості продовження життя в тому руслі, що було до 24го лютого 2022 року (наскільки це можливо).

Відзначаючи специфіку електронних договорів, і враховуючи те, що важливим етапом укладення будь-якого договору є його підписання, зазначимо, що при укладенні договорів у цифровій (електронній) площині важливе значення має питання щодо ідентифікації особи. Під такою ідентифікацією законодавець розуміє процедуру використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті

виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи, де ідентифікаційними даними особи є унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи¹. Враховуючи особливості ІТ середовища, будь-яка правова дія в електронній площині не може обійтися без ідентифікації.

Закон України «Про електронні довірчі послуги» (ст. 15) визначає, що схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Нині генерування електронного підпису може зайняти декілька хвилин, що досить зручно та позитивно впливає на швидкість вчинення відповідних юридичних дій. Така ситуація дала можливість розширити перелік ситуацій, де може бути застосовано електронний підпис. Наприклад, в освітньому процесі така можливість використовується під час укладення договору про надання освітніх послуг, прийняття заліків та іспитів у здобувачів вищої освіти, подачі за загальний розгляд свого дисертаційного дослідження майбутнім доктором філософії тощо. Особливо важливим ідентифікація викладачів, які здійснюють навчальний процес в умовах воєнного стану далеко від дому, не мають фізичної можливості знаходитися в закладі освіти, де вони працюють. Це дає можливість не припиняти надання освітніх послуг, не втрачати як викладачів (яким необхідно мати заробіток та можливість кормити свою сім'ю), так і здобувачів освіти.

Отже, навіть якщо особа фізично не знаходиться на території України, вона може продовжувати працювати, навчатися, бути активним учасником цивільно-правових відносин, укладати договори та виконувати їх тощо.

Разом з тим, не можна забувати й про недоліки цифровізації, зокрема, можливість зламу системи, отримання доступу злочинцями, шахраями тощо до «закритої» інформації. Така ситуація мала місце і при роботі з Єдиним державним веб-порталом електронних послуг «Дія» (стався витік персональних даних і їх відкриття для публічного ознайомлення). Маємо надію на те, що розвиток технологій та збіль-

¹ Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19>

шення спеціалістів в галузі кібербезпеки буде позитивно впливати на рівень захисту інформації, в тому числі, персональних даних.

Отже, «в центрі» будь-яких суспільних (а отже, і цивільних) відносин є приватні особи, суб'єкти приватного права, учасники цивільних відносин, що має враховуватися при формуванні норм і правил приватного (цивільного) права, які визначають взаємини членів суспільства одне з одним і з державою, як суб'єктом приватних відносин. Дані питання не втрачають своєї актуальності і в умовах воєнного стану (війни). Зокрема, на практиці виникає чимало проблем в даному напрямку. Якщо ж говорити більш конкретно, зокрема, стосовно вчинення та виконання правочинів в даних умовах, то необхідно зазначити, що досить велика кількість зобов'язань не виконуються в строк або ж не виконуються взагалі. Також постає питання про суб'єктний склад укладених правочинів. Адже Україна впродовж війни, яка триває вже більше півроку, втратила багато людей, кожен з яких мав свої приватно-правові зобов'язання, і не завжди є фізична можливість (знаходження в іншій країні, в регіонах активних бойових дій, в полоні тощо) та юридичне обґрунтування (доведення правонаступництва, представлення законних інтересів тощо) виконати зобов'язання. Звичайно, війна це форс-мажорна обставина, що позитивно вплине на результат більш пізнього виконання зобов'язань та не буде мати негативних наслідків у вигляді додаткових штрафних санкцій, однак глобально ситуація досить складна. Тут є і проблеми вчинення нових правочинів, наприклад, заповітів, дарування, договорів купівлі-продажу нерухомості тощо. Аналіз обмежень, які мали місце з початку війни в зазначених сферах, звичайно, є обґрунтованими з позиції публічного управління та прагнення держави захистити учасників цивільно-правових відносин від дій зловмисників (як то продаж нерухомості є неможливим без доступу до відповідних реєстрів; робота нотаріуса (в деяких випадках) є неможливою без входження його у спеціальний перелік нотаріусів, якими в умовах воєнного стану вчиняються нотаріальні дії щодо цінного майна¹ або ж якщо в даному регіоні ведуться бойові дії (внаслідок чого припинено доступ до єдиних та державних реєстрів) тощо).

¹ Мін'юстом затверджено перелік нотаріусів, якими в умовах воєнного стану вчиняються нотаріальні дії щодо цінного майна. URL: <https://www.kmu.gov.ua/news/minyustom-zatverdzheno-perelik-notariusiv-yakimi-v-umovah-voyennogo-stanu-vchinyayutsya-notarialni-diyi-shchodo-cinnogo-majna>

Підбиваючи підсумок можна впевнено стверджувати, що використання інформаційно-телекомунікаційних систем для вчинення правочинів розширює можливості як фізичних осіб, зокрема, дає можливість здійснювати необхідні дії, які забезпечують виникнення та припинення цивільних правовідносин, так і ФОП й юридичних осіб, зокрема, допомагає працювати та отримувати прибуток; все це в сукупності дає нам надію на забезпечення більш-менш нормального ритму життя особи в умовах воєнного стану та можливості захистити її цивільні права.

Підводячи підсумок необхідно зазначити, що у сучасних умовах збройного конфлікту та гібридних загроз, коли існує високий ризик втручання ворога в документообіг – як паперовий, так і традиційний електронний, – технологія блокчейн набуває особливої значущості. Її децентралізована, захищена від підробок і втручань структура забезпечує збереження достовірності юридично значущих дій навіть в умовах окупації, на тимчасово непідконтрольних територіях або в «сірій зоні». Це робить блокчейн ефективним інструментом для укладення договорів у критичних ситуаціях, коли традиційні форми правового оформлення втрачають надійність. Впровадження цієї технології може стати запорукою стабільності цивільно-правових відносин у періоди надзвичайної загрози.

Ключові слова: цивільне право, цивільні правовідносини, правочин, договір, IT-право, інформаційні технології, інформаційне суспільство, цифрова доба, гібридна війна, воєнний стан, соціальні мережі, смарт-контракт, блокчейн, штучний інтелект, відповідальність.