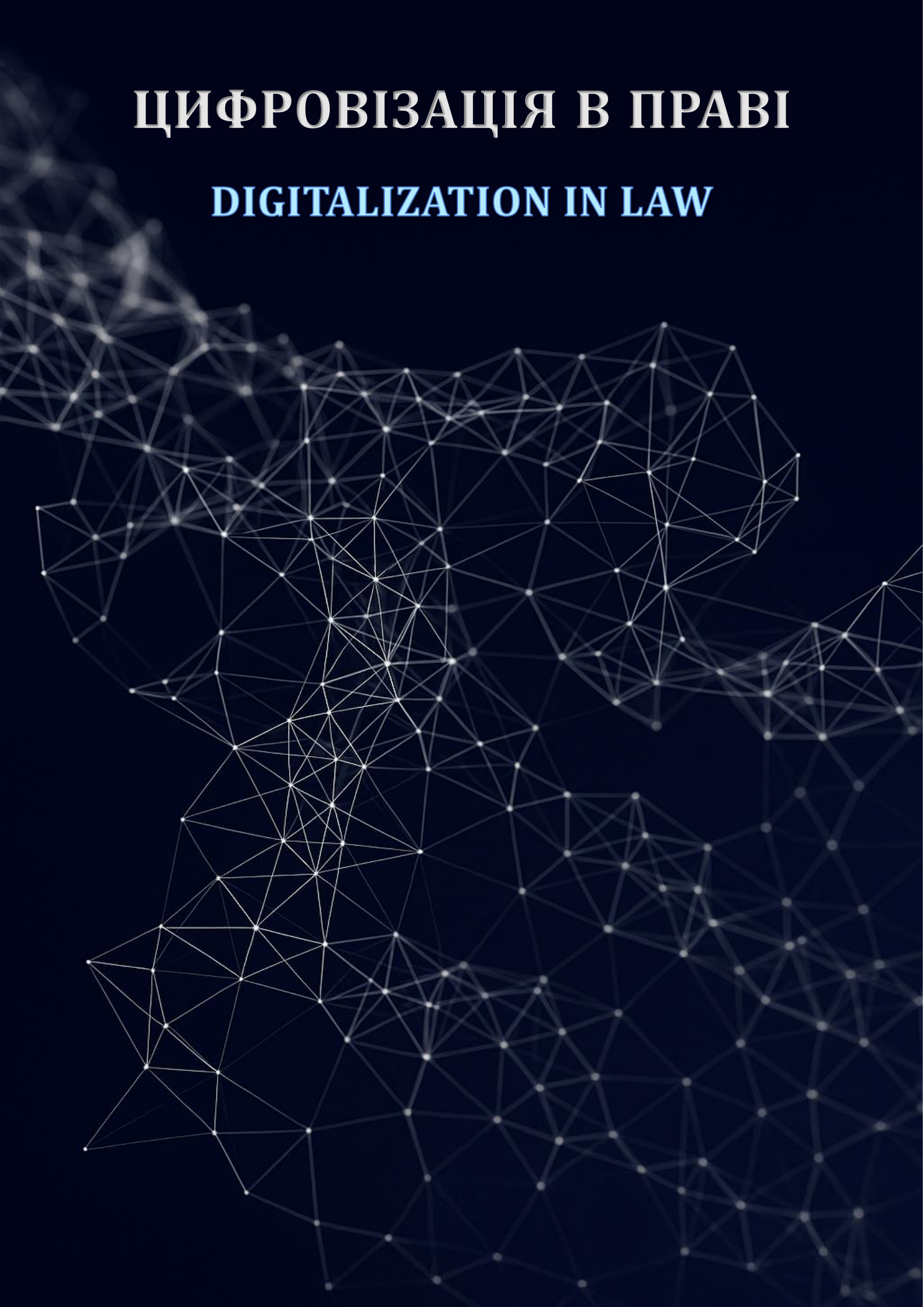


ЦИФРОВІЗАЦІЯ В ПРАВІ

DIGITALIZATION IN LAW



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

*С. Костенко, Ф. Мьосляйн, В. Стрільчук, Н. Пархоменко, Р. Ляшенко, І. Кравчук,
Д. Островський, Л. Василенко, Н. Бондарчук, Д. Оленюк, О. Радченко*

ЦИФРОВІЗАЦІЯ В ПРАВІ

Підручник

За редакцією кандидата юридичних наук,
доцента *С. Костенко*

Житомир 2025

УДК 34:004
Ц 75

*Рекомендовано до друку вченою радою Поліського національного
університету
(протокол № 10 від 28 травня 2025 р.)*

Р е ц е н з е н т и:

Олександр БАТАНОВ – доктор юридичних наук, професор, заслужений діяч науки і техніки України, провідний науковий співробітник відділу конституційного права та місцевого самоврядування Інституту держави і права імені В. М. Корецького НАН України;

Олексій ПІДДУБНИЙ – доктор юридичних наук, професор, завідувач кафедри цивільного та господарського права, Національний університет біоресурсів і природокористування;

Андрій ФЕДОРОНЧУК – кандидат юридичних наук, доцент, доцент кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника.

Ц75 Цифровізація в праві : підручник / С. Костенко, Ф. Мьосляйн, В. Стрільчук та ін. ; за ред. С. Костенко. Житомир : Поліський національний університет, 2025. 252 с.

ISBN 978-617-8410-04-9

Підручник охоплює широке коло питань, пов'язаних із цифровізацією у сфері права, зокрема нормативно-правові засади, технічні аспекти, міжнародний досвід та практичні кейси. Матеріал систематизовано за ключовими напрямками правового регулювання з використанням прикладів із юридичної практики, інтерактивних завдань і сучасних цифрових інструментів.

Видання призначене для студентів, викладачів, учнів, а також усіх, хто цікавиться правовими аспектами цифрової трансформації суспільства.

Підручник опубліковано на умовах ліцензії Creative Commons Із Зазначенням Авторства – Некомерційне Використання 4.0 Міжнародна (CC BY-NC 4.0).

Дозволено вільно копіювати, поширювати, змінювати та адаптувати цей матеріал за умови обов'язкового зазначення авторства.

Комерційне використання матеріалу суворо заборонено.

ISBN 978-617-8410-04-9

© С. Костенко, Ф. Мьосляйн, В. Стрільчук, Н. Пархоменко, Р. Ляшенко, І. Кравчук,
Д. Островський, Л. Василенко, Н. Бондарчук, Д. Оленюк, О. Радченко, 2025
© Поліський національний університет, 2025

ВІДОМОСТІ ПРО АВТОРІВ

Флоріан Мьосляйн (*Florian Möslein*)

Професор, доктор, LL.M. (Лондон),
Професор цивільного права, німецького
та європейського економічного права,
Інститут права цифровізації,
Філіппс-Університет м. Марбург (Німеччина)

Передмова

Наталія Пархоменко

Доктор юридичних наук, професор,
Інститут держави і права
ім. В.М. Корецького НАН України

Розділ I

Руслана Ляшенко

Кандидат юридичних наук, доцент,
Поліський національний університет

Розділ II

Світлана Костенко

Кандидат юридичних наук, доцент,
Поліський національний університет

Розділи III, VI, VII, VIII, XI (спільно з Радченко О.)

Даніель Островський (*Daniel Ostrovski*)

Докторант і науковий співробітник,
Інститут права цифровізації,
Філіппс-Університет м. Марбург (Німеччина)

Розділ IV

Леся Василенко

Кандидат юридичних наук, доцент,
Поліський національний університет

Розділ V

Наталія Бондарчук

Кандидат юридичних наук, доцент,
Поліський національний університет

Розділ IX

Дмитро Оленюк

Завідувач відділення бізнесу,
цифрових технологій та сервісу,
Житомирський кооперативний фаховий
коледж бізнесу і права;
Старший викладач кафедри комп'ютерних
технологій і моделювання систем,
Поліський національний університет

Розділ X

Олена Радченко

Кандидат юридичних наук, старший
викладач кафедри правознавства
Поліський національний університет,
адвокат

Віталій Стрільчук

Кандидат юридичних наук, доцент,
Поліський національний університет

Ірина Кравчук

Кандидат юридичних наук, доцент,
Поліський національний університет

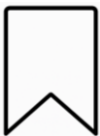
Розділ XI

(спільно з Костенко С.)

Розділ XII**Розділ XIII**

МЕТОДИЧНІ ТА ТЕХНОЛОГІЧНІ ЗАСАДИ ПІДРУЧНИКА

Підручник публікується як у паперовому, так і в електронному форматі. Електронна версія розповсюджується у комбінованій формі (індивідуально та через мережу). Для використання електронної версії підручника достатньо програми Adobe Acrobat. В електронній версії підручника зміст є гіпертекстовим, а робота з ним передбачає використання вказаних нижче кнопок і клавiш.

Значки	Дії
	У бічній панелі додатково доступний гіпертекстовий зміст, який відкривається після натискання на цей значок.
	Об'єкт з таким значком містить гіперпосилання на відео, яке відтворюється автоматично після натискання.
	Швидкий пошук слова у тексті, шляхом його введення у відповідне поле та натискання клавiші Enter.
 Колір тексту	Такий значок та/або колір тексту вказує на наявність гіперпосилання.

Під час підготовки цього підручника використовувалися такі цифрові інструменти як великі мовні моделі, зокрема ChatGPT, Gemini, Perplexity AI, а також Napkin AI. Мовні моделі застосовувались для генерації зображень, пошуку інформації та перефразування текстів. Уся зібрана інформація ретельно перевірялась авторами, які несуть персональну відповідальність за її достовірність.

ЗМІСТ

<i>ВІДОМОСТІ ПРО АВТОРІВ.....</i>	<i>3</i>
<i>МЕТОДИЧНІ ТА ТЕХНОЛОГІЧНІ ЗАСАДИ ПІДРУЧНИКА</i>	<i>5</i>
<i>ЗМІСТ.....</i>	<i>6</i>
<i>ПЕРЕДМОВА.....</i>	<i>10</i>
<i>Розділ I ВСТУП ДО ЦИФРОВІЗАЦІЇ В ПРАВІ.....</i>	<i>12</i>
1. Цифровізація у праві як вектор трансформації правової системи в умовах цифрової епохи	12
2. Виклики та перспективи цифровізації правової системи	13
Завдання	16
<i>Розділ II МЕТАВСЕСВІТ.....</i>	<i>18</i>
1. Поняття метавсесвіту та співвідношення з кіберпростором	18
2. Проблеми правового регулювання метавсесвіту	20
3. Значення метавсесвіту для юриста-практика та юридичної науки.....	25
Перевірка знань	29
Завдання	30
<i>Розділ III БЛОКЧЕЙН.....</i>	<i>31</i>
1. Поняття та принципи роботи блокчейну	31
2. Види та сфери застосування блокчейну	34
3. Право і блокчейн-технології	38
4. Досвід України щодо впровадження блокчейн-технологій	40
Перевірка знань	43
Завдання	44
<i>Розділ IV ТОКЕНИ.....</i>	<i>46</i>
1. Етимологія і зміст поняття „токен“	46
2. Типологія токенів: функціональні види та техніко-програмна база.....	48

2.1. Платіжні токени	50
2.2. Утилітарні токени	52
2.3. Токени активів, включаючи «security» - токени	53
2.4. Невзаємозамінні токени (NFT).....	56
3. Правові проблеми та виклики токенизації	58
3.1. Юридична природа tokenів	59
3.2. Юридичні невизначеності у сфері tokenів: потреба в системному врегулюванні	62
3.3. Супутні правові питання у контексті токенизації	67
Перевірка знань	67
Завдання	68
Розділ V SMART-КОНТРАКТИ.....	71
1. Поняття та сутність smart-контрактів: від ідеї до практики	71
2. Юридичний статус smart-контрактів.....	74
2.1. Співвідношення smart-контракту та традиційного цивільно-правового договору на сучасному етапі.	74
2.2. Перспективи застосування smart-контрактів у майбутньому в цивільних правовідносинах	75
2.3. Юридичне визнання smart-контрактів	78
2.4. Юрисдикція та міжнародний аспект застосування smart-контрактів ...	78
2.5. Проблеми щодо захисту порушених прав та інтересів користувачів smart-контрактів	79
3. Сфери застосування smart-контрактів.....	80
Перевірка знань	81
Завдання	82
Розділ VI ШТУЧНИЙ ІНТЕЛЕКТ.....	84
1. Поняття та основні форми штучного інтелекту.....	84
2. Інструменти ШІ в правовій сфері.....	89

3. Основні ризики використання ІІІ в юриспруденції та виклики для правового регулювання	91
4. Правове регулювання ІІІ в ЄС та Україні.....	93
Перевірка знань	100
Завдання	101
<i>Розділ VII ПРАВОВІ ТЕХНОЛОГІЇ.....</i>	103
1. Цифровізація юридичних послуг: проблематика дефініцій у контексті LegalTech та суміжних понять	103
2. LegalTech: значення, переваги та виклики	105
3. Типологія технологій LegalTech	111
4. Сучасні технології LegalTech: основні приклади	113
5. Правове регулювання LegalTech: міжнародний досвід.....	117
Перевірка знань	124
Завдання	125
<i>Розділ VIII ВЕЛИКІ МОВНІ МОДЕЛІ</i>	126
1. Базові терміни та принципи роботи	126
2. Класифікації LLM	133
3. Навички роботи з LLM як професійна необхідність юриста	138
Перевірка знань	139
Завдання	140
<i>Розділ ІХ ПРАВОВИЙ ДИЗАЙН.....</i>	143
1. Поняття та історія	143
2. Принципи правового дизайну.....	145
3. Етапи процесу правового дизайну	146
Перевірка знань	150
Завдання	151
<i>Розділ Х ПРОВА ІНФОРМАТИКА</i>	154
1. Теоретичні основи правової інформатики.....	154
2. Інформаційна безпека в юридичній діяльності	157

3. Хмарні технології у юридичній діяльності	160
4. Автоматизація роботи з юридичними документами	162
Перевірка знань	186
Завдання	187
<i>Розділ XI ЕЛЕКТРОННИЙ СУД.....</i>	189
1. Досвід України	189
2. Іноземний досвід.....	197
Перевірка знань	199
Завдання	200
<i>Розділ XII «РОЗУМНЕ» МІСТО.....</i>	201
1. Походження та становлення концепції „Smart City“	201
2. Еволюція змісту концепції „Smart City“	206
3. Політико-правовий вимір концепції „Smart City“	212
4. Значення Smart City для студентів-юристів	226
Перевірка знань	228
Завдання	229
<i>Розділ XIII ПРАВОВІ ОСНОВИ КІБЕРБЕЗПЕКИ.....</i>	231
1. Визначення поняття кібербезпеки.....	231
2. Правове регулювання кібербезпеки	233
3. Ключові загрози та властивості кібербезпеки	234
4. Кіберзлочинність : визначення, типи та методи боротьби	237
5. Доксинг	240
Перевірка знань	245
Завдання	246
<i>ПРЕДМЕТНИЙ ПОКАЖЧИК.....</i>	249

ПЕРЕДМОВА

Цифрова трансформація є визначальною ознакою нашого часу. Вона змінює фундаментальні процеси навчання, праці, комунікації – а також праворозуміння. Ці процеси не оминають права безслідно. Як система нормативного порядку, що має водночас забезпечувати гнучкість і стабільність, право постає перед завданням адекватно реагувати на цифрові виклики, не втрачаючи при цьому своїх основоположних принципів.

Підручник *Цифровізація в праві* пропонує системний аналіз ключових тенденцій на перетині права та цифрових технологій. У ньому досліджується, як правові системи трансформуються під впливом цифрових інновацій, і окреслюються підходи, які дозволяють юридичній освіті адекватно на це реагувати. Метою є підготовка нового покоління юристок і юристів, які володіють не лише фаховими юридичними знаннями, але й здатністю працювати з цифровими процесами, формувати нові правові підходи та зберігати стандарти прав людини й демократії у цифровому середовищі.

Цей підручник розглядається не лише як навчальний матеріал, а як інструмент для рефлексії над глибокими структурними змінами в правових системах – як в Україні, так і на міжнародному рівні. Цифровізація змінює не лише зовнішню форму, а й саму сутність правовідносин. Нові явища – такі як автоматизовані процедури ухвалення рішень, алгоритмічне правозастосування чи смарт-інфраструктури – ставлять правову науку перед питаннями, що вимагають міждисциплінарного та концептуально обґрунтованого осмислення.

Публікація є результатом міждисциплінарної та міжнародної співпраці. Вона об'єднує перспективи науковців і науковиць-юристів, а також практиків і практикинь з України та Німеччини, які досліджують правові аспекти цифровізації. Їхні внески відображають прагнення аналізувати правові процеси в міжнародному та порівняльному контексті.

Особлива увага у підручнику приділяється розвитку цифрової компетентності, здатності до критичного аналізу та міждисциплінарного мислення у студентів і молодих правників. У професійному середовищі, яке дедалі більше формують автоматизація та технічні системи, здатність поєднувати фахову правову компетентність з технологічним розумінням стає ключовою кваліфікацією. З метою підтримки цього підходу підручник створено в інтерактивному мультимедійному форматі – з гіперпосиланнями, вправами, інфографікою та кейс-аналізами, які спонукають до активного опрацювання матеріалу.

З огляду на підтримку міжнародної юридичної освіти та з урахуванням зростаючого значення англійської мови у фаховому дискурсі, підручник включає окремі англomовні елементи. Це полегшує інтеграцію у міжнародні освітні програми та сприяє розвитку вміння студентів впевнено працювати з іншомовними джерелами.

Публікація орієнтована на студентів, викладачів, практиків, а також усіх, хто цікавиться взаємодією між правом і технологіями – передусім тих, хто прагне долати складні виклики сучасності, поєднуючи юридичні знання, міждисциплінарну відкритість і суспільну відповідальність.

Флоріан Мьосляйн

*професор, доктор, LL.M. (Лондон),
професор цивільного права, німецького
та європейського економічного права,
Інститут права цифровізації,
Філіппс-Університет м. Марбург (Німеччина)*

Розділ I ВСТУП ДО ЦИФРОВІЗАЦІЇ В ПРАВІ **INTRODUCTION TO DIGITALIZATION IN LAW**

1. Цифровізація у праві як вектор трансформації правової системи в умовах цифрової епохи

У ХХІ столітті цифровізація стала однією з провідних тенденцій розвитку суспільства, істотно впливаючи на всі сфери його функціонування, включаючи правову. Цифрові технології змінюють не лише способи комунікації, управління та ведення бізнесу, а й саму природу правових відносин, механізми правозастосування та форми захисту прав людини.

Цифровізація у праві охоплює широке коло питань: електронне правосуддя (e-justice), електронне урядування (e-government), правовий статус цифрових активів, кібербезпека, захист персональних даних, а також використання штучного інтелекту в юридичній практиці. Ці зміни вимагають нових теоретичних підходів, перегляду чинного законодавства, а також формування цифрової правової культури.

В Україні цифровізація юридичної діяльності набула особливої актуальності після впровадження стратегії цифрової трансформації та розвитку проекту «Держава у смартфоні», реалізованого в межах діяльності Міністерства цифрової трансформації. У 2020 році було ухвалено Закон України «Про електронні довірчі послуги», а також розпочато активну цифрову модернізацію судової системи, зокрема впровадження Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС).

У сучасному глобалізованому світі цифровізація стала ключовим чинником трансформації суспільства, впливаючи на всі аспекти державного управління, економіки, соціального життя та правової системи. В умовах інформаційного суспільства особливої актуальності набуває питання цифрової трансформації у сфері права, що включає як модернізацію правового регулювання, так і цифровізацію юридичної практики.

Цифровізація у праві – процес, що забезпечує ефективне впровадження цифрових рішень в діяльність органів державної влади, правотворення, правозастосування та доступу громадян до правосуддя.

Правове забезпечення цифрової трансформації в Україні передбачає адаптацію національного законодавства до умов цифрової епохи, гармонізацію з міжнародними стандартами, а також врахування нових правових категорій, таких як «цифрова держава», «електронна демократія», «інформаційна безпека» тощо¹.

Водночас цифрові технології стають потужним інструментом оптимізації юридичної діяльності, але водночас породжують нові ризики – зокрема, в сфері кібербезпеки, збереження конфіденційності даних, юридичної відповідальності за автоматизовані рішення².

Таким чином, цифровізація в праві виступає не лише як технологічна модернізація, але і як глибока трансформація правової думки та інституцій. Це вимагає переосмислення класичних правових категорій, створення нових регуляторних механізмів та формування цифрової правової культури.

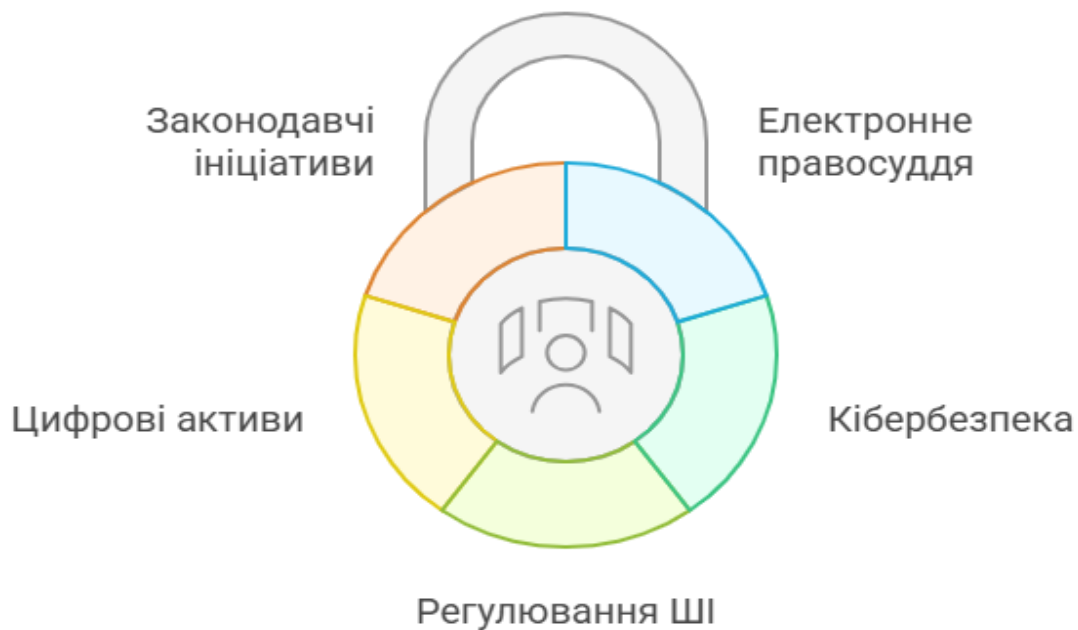
2. Виклики та перспективи цифровізації правової системи

У сучасному глобалізованому світі цифровізація стала не просто трендом, а визначальним чинником трансформації правових систем. Впровадження цифрових технологій змінює сутність юридичної практики, способи реалізації та захисту прав, а також функціонування державних інституцій. Цифровізація у праві є відповіддю на виклики інформаційного суспільства та необхідністю адаптації права до нових реалій.

¹ Лупенко В. Р., Пікуля Т. О., Еннан Р. Є. *Правове забезпечення цифрової трансформації в Україні. Науковий вісник Ужгородського національного університету*. Серія: Право. 2022. № 72. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/300456/292764> (дата звернення: 10.04.2025).

² Перехід до цифрових рішень: юридичний ринок і виклики цифровізації. *Юридична газета*. 2023. URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/perehid-do-cifrovih-rishen-yuridichniy-rinok-i-vikliki-cifrovizaciyi.html> (дата звернення: 10.04.2025).

Вплив цифровізації на правову систему України



Цифровізація права вимагає переосмислення ряду фундаментальних правових категорій, зокрема:

- **Джерела права** – зростає значення електронних актів, онлайн-платформ як засобів офіційного оприлюднення;
- **Правосуб'єктність** – з'являються нові учасники правових відносин, такі як штучний інтелект;
- **Форми правозастосування** – електронне правосуддя, автоматизовані рішення в адміністративному процесі;
- **Докази** – цифрові докази, їх достовірність, зберігання та допустимість у судовому процесі.

Україна демонструє активне впровадження цифрових технологій у правову сферу. Зокрема, створення та розвиток проєкту «Дія» та платформи «Дія. Цифрова держава», функціонування Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), електронне декларування, електронні довірчі послуги згідно із Законом України «Про електронні довірчі послуги» №2155-VIII.

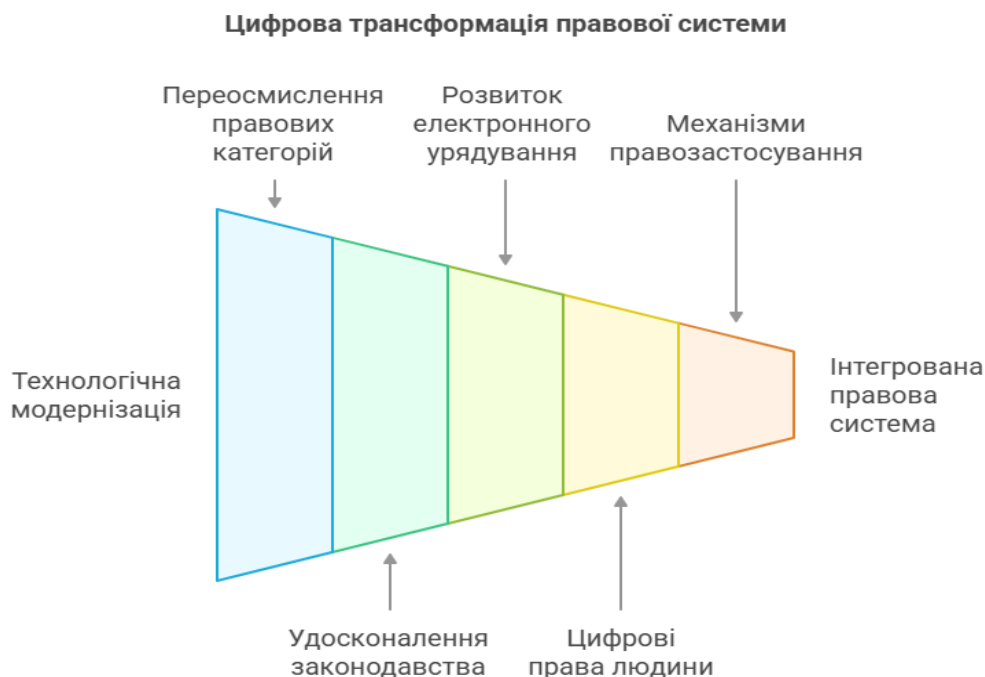
Європейський Союз активно розвиває правову рамку для цифрового середовища. Важливими документами є:

- **General Data Protection Regulation (GDPR)** – регламентує обробку персональних даних;
- **AI Act** – регулює використання систем штучного інтелекту;
- **Digital Services Act** та **Digital Markets Act** – забезпечують правовий порядок в інтернет-просторі.

Ці документи впливають на формування української правової політики у сфері цифровізації, оскільки Україна прагне до правової гармонізації з ЄС.

Серед основних викликів:

- **відсутність єдиного цифрового правового словника**, що ускладнює уніфікацію термінології в законодавстві та правозастосуванні.
- **ризик порушення прав людини** внаслідок використання автоматизованих рішень, зокрема щодо персональних даних, приватності, права на справедливий суд.
- **проблеми кібербезпеки та захисту інформаційних систем**, особливо в умовах збройного конфлікту та гібридних загроз.
- **цифрова нерівність** — не всі верстви населення мають доступ до цифрових правових послуг, що призводить до обмеження доступу до правосуддя.



Отже, цифровізація в праві — це не просто технологічна модернізація юридичної діяльності, а **системна трансформація правового мислення**, яка охоплює переосмислення правових категорій, удосконалення законодавства, розвиток електронного урядування, цифрових прав людини та механізмів правозастосування.

Україна впевнено рухається у напрямку цифрової трансформації, що вимагає активної участі наукової спільноти, законотворців та юристів-практиків у створенні гнучкої, надійної та інноваційної правової системи, здатної відповідати викликам сучасності.



ЗАВДАННЯ



1. Debate: «Digital State – Risks or New Opportunities?»

Формат: коротке есе (до 2 сторінок) або участь у дебатах в аудиторії/онлайн.

Questions:

- Чи забезпечує цифрова держава кращий захист прав людини?
- Як уникнути зловживань з боку держави в умовах цифровізації управління?
- Які цифрові інструменти могли б забезпечити прозорість та довіру до правової системи?



2. Creative Assignment: «Digital Rights in the 21st Century»

Формат: інфографіка / презентація / постер.

Questions:

- Що таке цифрові права?

- Які нові права людини виникають у цифрову епоху (право на забуття, цифрове громадянство тощо)?
- Як законодавство України враховує ці права?



3. Interactive Survey: «Digital Court – Pros and Cons»

Проведіть опитування у Google Forms або Mentimeter та підготуйте короткий звіт з аналізом результатів і власними висновками.

Survey questions:

- Чи довіряєте ви онлайн-слуханням у суді?
- Чи має штучний інтелект право ухвалювати судові рішення?



4. Practical Assignment: «Legal Analysis of a Digital Law Act»

Оберіть один із законодавчих актів та проведіть юридичне дослідження (1–2 сторінки), коротко охарактеризувавши зміст та визначивши значення відповідного нормативно-правового акта для правової системи України в цифрову епоху.

👉 Закон України «Про електронні довірчі послуги»

👉 Закон України «Про цифровий контент та цифрові послуги»

👉 Регламент GDPR

Розділ II METABCECBIT METAVERSE

1. Поняття метавсесвіту та співвідношення з кіберпростором



Метавсесвіт (англ. *metaverse*) – це особливий віртуальний простір, створений за допомогою цифрових технологій, у якому користувачі взаємодіють між собою та з цифровим середовищем через свої аватари – віртуальні двійники. Іншими словами,

метавсесвіт є своєрідною цифровою копією реального світу, що існує в мережі Інтернет. У цьому інтерактивному просторі поєднано сучасні інноваційні технології – віртуальну (VR) та доповнену (AR) реальності, тривимірну графіку, штучний інтелект (AI), блокчейн та криптовалюти, соціальні мережі тощо. Завдяки цьому метавсесвіт забезпечує ефект занурення і постійної присутності, дозволяючи у цифровому світі спілкуватися, працювати, навчатися, укладати угоди, створювати та відчужувати об’єкти, розважатися.

Термін «*metaverse*» уперше з’явився у науковій фантастиці – в романі Ніла Стівенсона «*Snow Crash*» (1992), де описано віртуальний світ майбутнього. Ще раніше використовувалося поняття «кіберпростір» (англ. *cyberspace*), запроваджене Вільямом Гібсоном у романі «*Neuromancer*» (1984) для позначення уявного цифрового простору³.

Сьогодні поняття метавсесвіту не має усталеного юридичного визначення і трактується по-різному. Деякі дослідники вважають метавсесвіт наступним

³ Сverdlichenko V.P. Метавсесвіт – майбутній простір дослідження для юриспруденції. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2024. Випуск 81. Частина 2. С. 223.

етапом еволюції Інтернету (так званого Інтернету нового покоління або Web 3.0) – перетворенням глобальної мережі з двовимірних сайтів на «живий» тривимірний світ. У популярній літературі метавсесвіт часто ототожнюють із віртуальною реальністю загалом. Втім, у науковому дискурсі все частіше підкреслюється, що метавсесвіт – більш комплексне явище, ніж окремі VR/AR-технології чи онлайн-ігри, оскільки становить єдину постійну віртуальну систему, потенційно спільну для необмеженої кількості користувачів і сумісну між різними платформами.



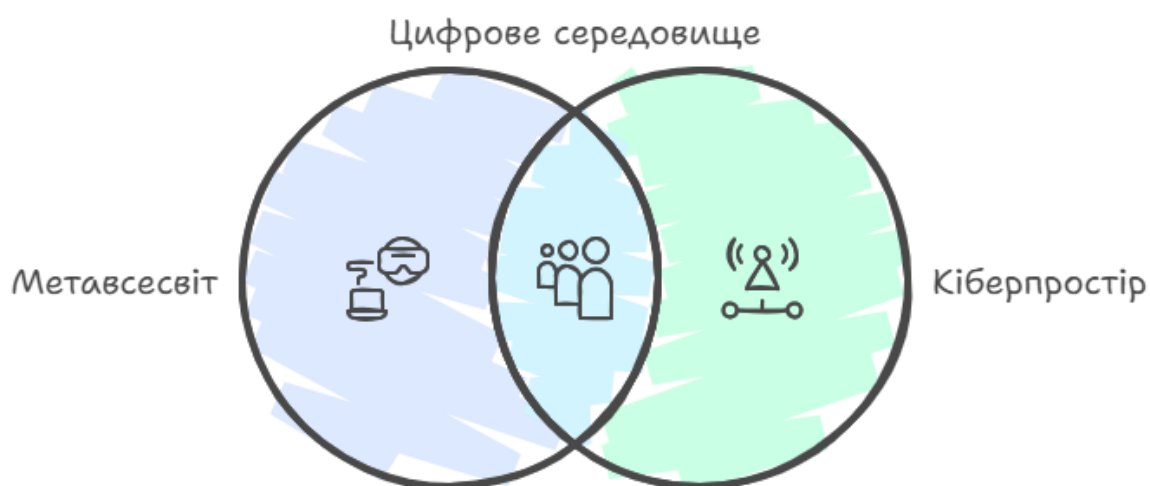
МЕТАВСЕСВІТ VS КІБЕРПРОСТІР

Питання співвідношення метавсесвіту з ширшим поняттям кіберпростору є дискусійним.

З одного боку, метавсесвіт можна розглядати як частину або форму кіберпростору, адже це різновид цифрового середовища, що функціонує на базі Інтернету. Інформаційні правовідносини, які виникають у віртуальній реальності метавсесвіту, загалом підпадають під категорію правовідносин у кіберпросторі. З іншого боку, між цими поняттями можна виокремити принципові відмінності. По-перше, метавсесвіт передбачає вищий рівень імерсивності (занурення) та присутності, ніж традиційний кіберпростір: користувач не просто споживає

інформацію, а діє від імені свого аватара у тривимірному середовищі, наближеному до реальності. По-друге, метавсесвіт орієнтований на створення єдиного віртуального світу, що може об'єднати різні платформи та сервіси, тоді як кіберпростір – поняття ширше, яке охоплює всі мережеві взаємодії (від вебсайтів до електронної пошти) і не є цілісним «світом».

Перетворення цифрового середовища



Отже, метавсесвіт є частиною кіберпростору, його новітнім втіленням, що має власні специфічні риси.

2. Проблеми правового регулювання метавсесвіту

Стрімкий розвиток метавсесвіту породжує численні юридичні виклики. Наразі не розроблено спеціальних правових норм, що регулюють відносини у віртуальних світах, відповідні законодавчі акти лише починають з'являтися в окремих державах. Відтак, на порядок денний виходить адаптація існуючих правових інститутів до нових цифрових реалій. Розглянемо основні напрямки правового регулювання актуальні для метавсесвіту⁴.

⁴ Woodford I. Colombia court moves to metaverse to host hearing. URL: <https://www.reuters.com/world/americas/colombia-court-moves-metaverse-host-hearing-2023-02-24/#:~:text=At%20the%20two,dressed%20in%20black%20legal%20robes> (date of access: 17.03.2025).

Юрисдикція. Одним із перших питань, з яким стикаються учасники метавсесвіту, є визначення юрисдикції: право якої держави регулює відносини у цьому глобальному цифровому просторі. Метавсесвіт не має чіткої територіальної прив'язки, користувачі можуть перебувати в різних країнах, сервери розосереджені по всьому світу. Це ускладнює використання традиційних колізійних прив'язок (території вчинення дії, місця знаходження майна тощо). Виникає ідея формування **електронної юрисдикції** метавсесвіту – умовного правового простору, правила якого визнаються більшістю учасників незалежно від їх належності до держави. Наразі відсутність визначеності у питанні юрисдикції спричиняє правову невизначеність: навіть якщо обрати право певної країни, її закони зазвичай не пристосовані до віртуальних середовищ і не дають чітких відповідей на специфічні проблеми які виникають у середовищі метавсесвіту.

Захист персональних даних. Метавсесвіт оперує безпрецедентними обсягами персональних даних. Кожна дія аватара, кожен об'єкт чи локація можуть збирати дані про користувача. До того ж використовуються біометричні дані (наприклад, відстеження рухів очей, міміки, фізіологічних параметрів у VR-гарнітурах) – усе це чутлива інформація, яка потребує захисту. Тому на перший план виходить застосування законодавства про захист даних (GDPR в ЄС ⁵, Закон України «Про захист персональних даних»⁶ тощо) у контексті метавсесвіту. Виникають питання: як отримувати згоду користувача на обробку такої детальної інформації, чи може провайдер метавсесвіту збирати та передавати ці дані третім особам, як забезпечити право на приватність у середовищі постійного моніторингу? Вже зараз експерти застерігають про ризики неконтрольованого збору персональних даних у метавсесвіті.

⁵ Загальний регламент про захист даних: Європарламент, Рада ЄС; Регламент, Міжнародний документ від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 27.03.2025).

⁶ Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 27.03.2025).

Цифрова ідентичність та аватари. У метавсесвіті кожна фізична особа представлена цифровими персонажами. Постає проблема правового статусу такого аватара та пов'язаного з ним поняття **цифрової особистості**. Зокрема, потрібно вирішити: як ідентифікувати користувачів (чи повинні вони проходити верифікацію, щоб підтвердити, хто керує аватаром), чи можуть створюватися автономні аватари на основі ШІ без прямого контролю людини, і хто несе відповідальність. Відомим є термін «електронний кіднепінг» – незаконне заволодіння аватаром або цифровим двійником особи без її згоди. Така ситуація може призвести до шахрайства або навіть використання викраденого аватара для протиправних дій, зокрема для скоєння терористичних актів⁷. Це потребує врегулювання на законодавчому рівні цифрової ідентичності користувача, надійної захищеності інформації. Також необхідно визначити, чи має аватар окремі права (наприклад, право «на життя» у віртуальному просторі) чи всі дії аватара розглядаються як дії відповідної фізичної особи.

Інтелектуальна власність. Метавсесвіт вже зараз стає полем для порушень авторського права та суміжних прав, торговельних марок, патентів тощо. У віртуальному середовищі можуть відтворюватися реальні об'єкти, твори, бренди без дозволу власників. Приміром, іспанський бренд одягу Mango відтворив твори відомих іспанських художників у метавсесвіті без дозволу власників. Суд у Барселоні став на бік Mango, визнавши, що компанія не порушила авторських прав, оскільки мала право на трансформацію та інновації цих творів у віртуальному середовищі⁸. Інший кейс – французький модний дім Hermès подав позов проти цифрового художника Мейсона Ротшильда за створення та продаж NFT під назвою «MetaBirkin», які зображували сумки, схожі на відомі сумки Birkin. Hermès стверджував, що це порушує їхні права на торговельну марку. У лютому 2023 року суд присяжних визнав Ротшильда винним у порушенні прав

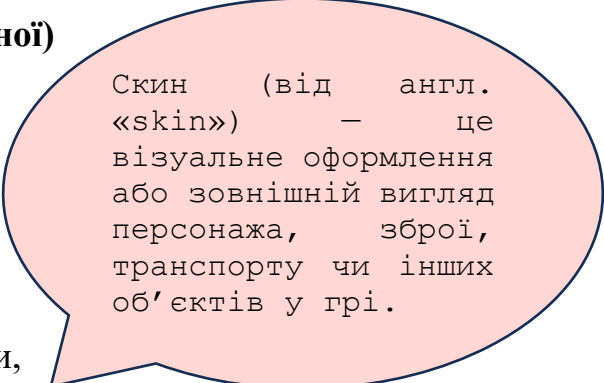
⁷ Палій. А. Закони майбутнього: чого чекати від регулювання метавсесвіту. Юридична газета online. 2023. №7–8 (765–766). URL: <https://jur-gazeta.com/publications/practice/informaciynе-pravo-telekomunikaciyi/zakoni-maybutnogo-chogo-chekati-vid-regulyuvannya-metavsesvitu-.html> (дата звернення: 27.03.2025).

⁸ White & Case secures dismissal for Mango in cutting-edge metaverse art dispute. URL: https://www.whitecase.com/news/press-release/white-case-secures-dismissal-mango-in-cutting-edge-metaverse-art-dispute?utm_source=chatgpt.com (date of access:: 27.03.2025).

на торговельну марку, присудивши Hermès 133 000 \$ компенсації⁹. Такі кейси порушують питання: хто і яку несе відповідальність за порушення права інтелектуальної власності в метавсесвіті, яку юрисдикцію обрати для захисту прав, як кваліфікувати саме цифрове правопорушення (копіювання об'єкта в VR тощо).

Віртуальні активи та віртуальна власність. У метавсесвіті виникає феномен **цифрової (віртуальної)**

власності – йдеться про об'єкти, що існують тільки у цифровій формі, але можуть мати цінність для користувачів: віртуальна земля чи будівлі, цифрові предмети (скини,



Скин (від англ. «skin») – це візуальне оформлення або зовнішній вигляд персонажа, зброї, транспорту чи інших об'єктів у грі.

аксесуари), валюти, токени. Юридично постає питання: чи визнавати за такими об'єктами статус майна і захист права власності на них. У деяких країнах зроблено перші кроки в цьому напрямі: так, Тайвань ще у 2001 році офіційно визнав, що об'єкти у віртуальних світах можуть розглядатися як майно, яке підлягає відчуженню¹⁰. В Україні також була спроба врегулювати це питання, детальніше про це дивитись на сторінці 37. Варто відзначити, що право віртуальної власності слід відрізняти від інтелектуальної власності та визначати як окремий вид речового права, об'єктом якого є саме цифрове майно, незалежно від його реального прототипу.

Кримінально-правові аспекти. Віртуальний простір метавсесвіту стає середовищем вчинення нових видів правопорушень. Уже зараз фіксуються інциденти протиправної поведінки аватарів: наприклад, випадки сексуальних домагань у VR-світах, кібербулінгу за допомогою аватарів, крадіжки цінних предметів із профілів користувачів. Постає питання про склад кримінального правопорушення у таких ситуаціях: як кваліфікувати такі діяння (скажімо,

⁹ Metaverse in case law: Hermès wins trademark infringement case over «MetaBirkin» NFTs. URL: https://preubohlig.de/newsletter/metaverse-in-case-law-hermes-wins-trademark-infringement-case-over-metabirkin-nfts/?lang=en&utm_source=chatgpt.com (date of access: 27.03.2025).

¹⁰ Joshua A.T. Fairfield (2005). Virtual property. *Boston University Law Review*. 2005. 1787. P. 1086. URL: <https://www.repository.law.indiana.edu/facpub/1787> (date of access: 27.03.2025).

«вбивство» аватара або знищення віртуального майна); кого притягувати до відповідальності. Якщо діє людина через свого аватара – відповідатиме вона (за умови встановлення особи, що стоїть за аватаром). Якщо ж автономний ШІ-аватар завдав шкоди – чи можна притягнути до відповідальності розробника програми або власника платформи? На сьогодні такі питання залишаються відкритими. Законодавство переважно реагує постфактум: кримінальні правопорушення у метавсесвіті кваліфікуються за наявними складами (наприклад, шахрайство, якщо було виманено криптовалюту; порушення недоторканності приватного життя, якщо зламано акаунт і викрадено дані). Однак, фахівці наголошують на потребі розробки модельних норм для метавсесвіту, тобто створення т. зв. «кодіфікованих правил».

Вирішення спорів. Традиційна судова система не пристосована до вирішення спорів, що виникають у метавсесвіті. По-перше, як зазначалось, важко визначити до суду якої юрисдикції належатиме спір, в якій державі здійснюватиметься судочинство. По-друге, розгляд справи судами окремої держави вимагає наявності спеціальних знань про цифрові технології, а виконання рішення у глобальному цифровому середовищі – окремий виклик. Тому провайдери метавсесвіту впроваджують власні механізми регулювання таких спорів. Наприклад, платформи можуть передбачати в угоді з користувачем, що спори між ними вирішуються шляхом онлайн-арбітражу за регламентом, визначеним самою платформою¹¹. З одного боку, це швидше та ефективніше для нескладних спорів, а з іншого – постає питання об'єктивності та законності таких «приватних судів». Наразі склалася ситуація, що значну частину питань у метавсесвіті врегульовано саме корпоративними правилами провайдерів (оферти, політики використання), а не на рівні національного чи міжнародного права. Це своєрідний приклад використання soft law – «м'якого права».

¹¹ Притика Ю. Д. Онлайн-арбітраж у системі альтернативних способів вирішення спорів: pro et contra. *Проблеми цивільного права та процесу*: тези доповідей учасників науково-практичної конференції, присвяченої світлій пам'яті Олександра Анатолійовича Пушкіна (25 травня 2018 р.). Харків, 2018. С. 59.

Правові виклики метавсесвіту



3. Значення метавсесвіту для юриста-практика та юридичної науки

Чому юристам важливо розуміти метавсесвіт? Метавсесвіт уже сьогодні з концепції перетворюється на практичну платформу для ведення бізнесу, надання послуг і соціальних взаємодій. За прогнозами, до 2030 року метаіндустрія може генерувати до 5 трлн доларів обороту. Більшість провідних компаній світу очікують, що розвиток метавсесвіту суттєво вплине на їх діяльність у найближчі 5–10 років¹². В цих умовах юристи-практики не можуть залишатися осторонь. З'являється запит на правовий супровід проєктів у метавсесвіті: від консультування IT-компаній щодо дотримання регуляторних вимог до допомоги креативним індустріям у захисті прав на цифровий контент. Юридичний бізнес все активніше досліджує можливості метавсесвіту:

¹² Meta-value. URL: <https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/meta-value> (date of access: 27.03.2025).

проведення віртуальних конференцій та зустрічей, маркетинг юридичних послуг через цифрові платформи.

Зміни у юридичній практиці. Впровадження нових технологій змінює і спосіб роботи правника. Уже нікого не дивує **електронний суд** чи онлайн-засідання. Наступний крок – це судові процеси з використанням VR-технологій, коли доказування або судовий розгляд відбувається за допомогою віртуальної реальності¹³. Наприклад, у 2023 р. в Колумбії відбулось перше судове засідання у метавсесвіті, де суддя і сторони були представлені аватарами (детальніше про це дивитись на с. 199)¹⁴. Крім того, щоденні юридичні завдання все більше автоматизуються: штучний інтелект уже застосовується для підготовки проєктів договорів, аналізу судової практики. У метавсесвіті ці процеси можуть прискоритися – з'являються т. зв. *«децентралізовані юридичні послуги»*, коли частину функцій юриста виконує алгоритм (наприклад, смарт-контракт автоматично фіксує права сторін і штрафні санкції)¹⁵. Юристу варто не боятися таких змін, а використовувати їх: навчитися співпрацювати з IT-фахівцями, контролювати результати роботи алгоритмів, перевіряти коректність закладеної у них логіки та інформації.

Нові виклики та етичні дилеми. Поєднання права і метавсесвіту ставить перед юристами низку **етичних питань**. Як забезпечити конфіденційність адвокатської таємниці під час спілкування у VR, якщо провайдер теоретично може відстежувати усе, що відбувається? Чи не порушує законодавство роботодавець, коли контролює пересування і дії аватара свого працівника в робочому метавсесвіті поза робочим часом (аватар працівника часто асоціюється з брендом компанії і якщо такий аватар у метавсесвіті бере участь у небажаних

¹³ Костенко С. О. VR-технології як новий вимір доказування: виклики для України та юридичної освіти. Theoretical and empirical scientific research: concept and trends: Collection of scientific papers «ΛΟΓΟΣ» with Proceedings of the VIII International Scientific and Practical Conference, Oxford, March 7, 2025 / Oxford-Vinnytsia: P.C. Publishing House & UKRLOGOS Group LLC, 2025. С.116-118. DOI 10.36074/logos-07.03.2025.023

¹⁴ Woodford I. Colombia court moves to metaverse to host hearing. URL: <https://www.reuters.com/world/americas/colombia-court-moves-metaverse-host-hearing-2023-02-24/#:~:text=At%20the%20two,dressed%20in%20black%20legal%20robes> (date of access: 17.03.2025).

¹⁵ VAIOT's DeLaw Ecosystem: Tools that are bringing decentralization to the Legal Landscape in 2024 URL: <https://vaiotltd.medium.com/vaiots-delaw-ecosystem-tools-that-are-bringing-decentralization-to-the-legal-landscape-in-2024-0597e3784b12> (date of access: 17.03.2025).

чи неетичних діях, то це може вплинути на імідж компанії)? Відповіді на ці питання не завжди очевидні та вимагають розробки нових стандартів професійної етики та законодавчого регулювання.

Вплив на правничу науку. Для правничої науки метавсесвіт відкриває новий простір для досліджень: правове регулювання штучного інтелекту, правова природа віртуального майна, співвідношення реальних і цифрових прав тощо. Вже зараз науковці розробляють понятійно-категоріальний апарат для опису явищ метавсесвіту мовою права. З'являються наукові праці¹⁶, присвячені юридичним аспектам метавсесвіту. Особливо динамічно розвиваються міждисциплінарні дослідження. Для комплексного розв'язання проблем, що виникають у цифровому світі, юристам доводиться працювати спільно з філософами (переосмислення поняття реальності, цінностей, особистості у віртуальному середовищі), соціологами (вивчення поведінки спільнот у метавсесвіті), психологами (вплив VR на свідомість і волю людини), фахівцями з кібербезпеки (захист від нових загроз). Таким чином, правнича наука реагує на появу метавсесвіту розширенням методології наукових досліджень, залученням крос-дисциплінарних підходів.

Освіта та підготовка кадрів. Важливим аспектом є пристосування **юридичної освіти** до нових реалій. Уже зараз провідні університети світу вводять спецкурси, присвячені цифровізації права, криптовалютам, кібербезпеці¹⁷. Логічним кроком є поява курсів з права метавсесвіту, де студенти-правники вивчатимуть кейси, пов'язані з VR, відпрацьовуватимуть навички онлайн-взаємодії. В Україні такі курси тільки починають формуватися, однак попит на них зростає. Юрист майбутнього, ймовірно, повинен буде володіти базовими ІТ-навичками, розуміти принципи роботи блокчейну, розбиратися в питаннях інформаційної безпеки. Окрім того, знадобляться

¹⁶ Костенко О. В., Головка О. М. Електронна юрисдикція Metaverse: виклики та ризики правового регулювання віртуальної реальності. *Інформація і право*. 2023. № 1 (44). С. 105–115; Ващак В. А. Саморегулювання цивільних відносин в інтернеті: дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. Національний університет «Одеська юридична академія», МОН України, Одеса, 2024. 244 с.

¹⁷ Костенко С.О. Феномен права цифровізації та його вплив на юридичну освіту. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. №2. С.54-60. DOI: 10.24144/2788-6018.2025.02.6

«м'які» навички для роботи в новому середовищі – гнучкість, здатність швидко навчатися, креативність у пошуку рішень.

Юридичні можливості в цифрову епоху

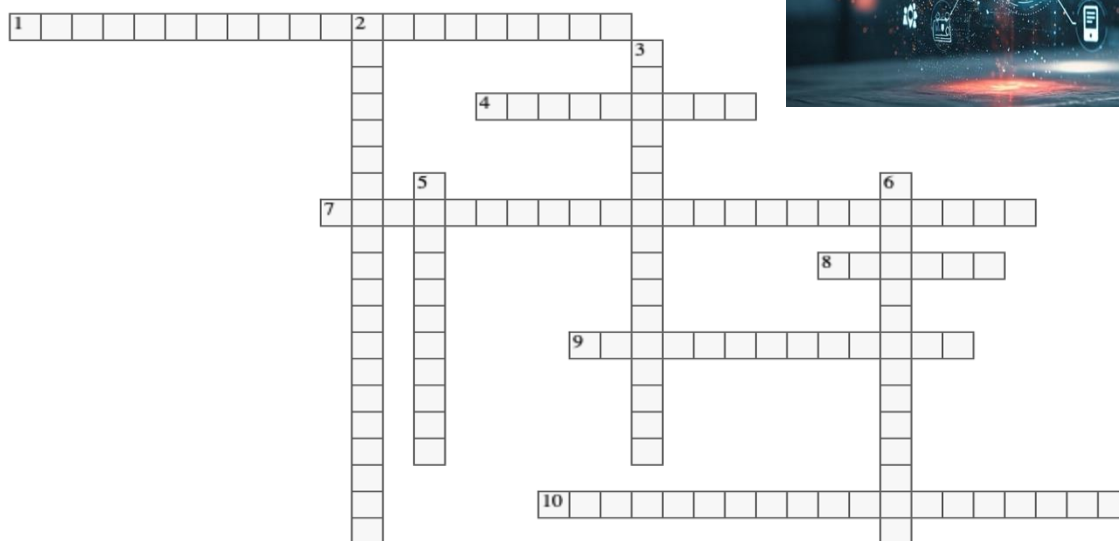


Підсумовуючи, потрібно зазначити, що на сучасному етапі правове регулювання суттєво відстає від технологічних інновацій. Правові аспекти метавсесвіту набувають все більшого значення як для практикуючих юристів, так і для науковців-правників. Практики повинні адаптувати свої компетенції аби ефективно захищати права клієнтів у віртуальному світі. Наука ж має виконати важливу місію – підготувати теоретичне підґрунтя і пропозиції для

нормативного регулювання метавсесвіту. Юристам майбутнього доведеться опановувати нові компетенції, а законодавцям – шукати баланс між свободою цифрових світів та необхідністю захисту прав і інтересів їх учасників. Формування міжнародних стандартів та співпраця держав будуть ключовими факторами успіху у впорядкуванні метавсесвіту як простору, що вже перестає бути фантастикою і стає частиною повсякденного життя.

ПЕРЕВІРКА ЗНАНЬ

Для закріплення пройденого матеріалу розв'яжіть кросворд. Деякі відповіді складаються з двох слів – вони записуються без пробілу, якщо з апострофом – без нього, якщо з дефісом – без нього.



По горизонталі

1. Технологія, яка забезпечує занурення у віртуальний світ.
4. Юридичне поняття, яке визначає правила поведінки в цифровому середовищі без обов'язкової сили.
7. Галузь права, яка захищає інновації, контент, бренди.
8. Термін, яким позначають цифрового двійника користувача у метавсесвіті.
9. Правовий механізм, який дозволяє користувачу укладати угоди у віртуальному середовищі автоматично.
10. Тип реальності, яка поєднує елементи цифрового і фізичного світів.

По вертикалі

2. Термін для позначення незаконного заволодіння аватаром.
3. Грошовий чи ціннісний об'єкт, який існує лише у віртуальному просторі.
5. Процедура підтвердження справжності особи у цифровому середовищі.
6. Форма електронного альтернативного вирішення спорів.

ЗАВДАННЯ

**1. Discussion: «Metaverse & Law – Regulate or Let It Evolve?»**

Напишіть коротке есе (an essay) на тему: *чи потрібне спеціальне правове регулювання метавсесвіту на міжнародному чи національному рівні?*

Questions:

- Яка модель юрисдикції може бути ефективною для метавсесвіту?
- Чи потрібно створювати міжнародний кодекс поведінки (наприклад, «Цифрову конвенцію метавсесвіту»)?
- Яка роль soft law у регулюванні метавсесвітів?

**2. Case Study «Hermès v. Rothschild»**

Проаналізуйте судовий кейс **Hermès v. Mason Rothschild**¹⁸ пов'язаний з метавсесвітом у формі аналітичної записки (до 2 сторінок), розкривши наступні пункти:

- Фактичні обставини справи
- Аргументи сторін
- Юридична проблема

**3. Експрес-опитування: «Чи довіряєш метавсесвіту?»**

Проведіть онлайн-опитування серед студентів/друзів на тему: *«Чи погодилися б ви укласти трудовий договір у метавсесвіті через свого аватара?»*

Підготуйте короткий звіт із висновками (можна у вигляді презентації або постера).

¹⁸ WIPO Lex WIPOLEX038-j. United States District Court of the Southern District of New York [2023]: Hermes Int'l v. Rothschild, No. 22-CV-384-JSR, 2023 WL 1458126 (S.D.N.Y. Feb. 2, 2023). URL: <https://www.wipo.int/wipolex/en/text/588771> (date of access: 17.03.2025).

Розділ III БЛОКЧЕЙН

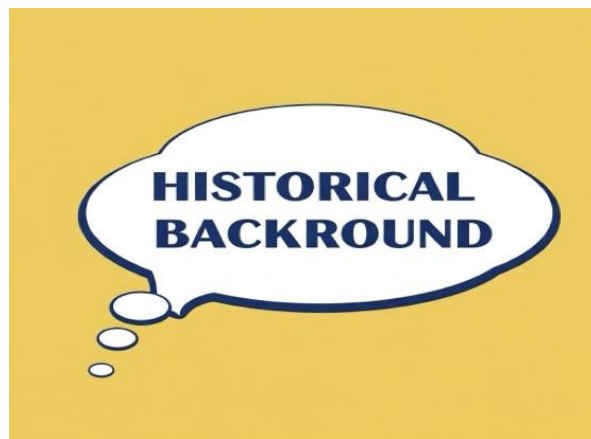
BLOCKCHAIN

1. Поняття та принципи роботи блокчейну

Ідейні основи блокчейну були закладені ще в 1990-х роках у працях різних науковців у сфері криптографії. Однак лише у 2008 році було опубліковано статтю «*Bitcoin: A Peer-to-Peer Electronic Cash System*»¹⁹, в якій невідома особа або група осіб під

псевдонімом **Сатоші Накамото (Satoshi Nakamoto)** змогла об'єднати попередні досягнення науковців у цій сфері та розробити концепцію блокчейну. Перше реальне застосування блокчейну відбулося у 2009 року з появою Біткойна.

Варто відзначити, що запуск Біткойна відбувся після глобальної економічної кризи 2008 року, яка призвела до масових банкрутств компаній, скорочення бізнесу, зростання безробіття та падіння державних доходів. Хоча ідея децентралізованих цифрових грошей існувала ще до цієї кризи, саме недовіра до традиційної фінансової системи стала каталізатором для створення Біткойна – валюти, що не залежить від банків і урядів.



Blockchain (англ. від block – блок, chain – ланцюг, тобто ланцюжок блоків) – розподілена база даних, що зберігає впорядкований ланцюг записів (так званих блоків), який постійно довшає²⁰.

¹⁹ Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: <https://bitcoin.org/bitcoin.pdf> (date of access: 17.03.2025).

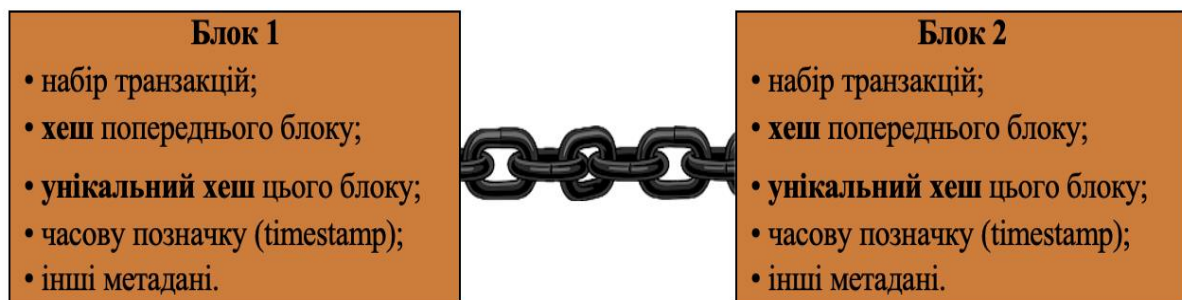
²⁰ The great chain of being sure about things. *The Economist*. URL: <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> (date of access: 17.03.2025).

Іншими словами блокчейн також називають **реєстром**, який використовується для зберігання записів у вигляді блоків, які пов'язані між собою криптографічно. Його головна особливість – це незмінність даних після запису, що робить його стійким до підробок і змін.

Такий реєстр є **розподіленим**, що означає його зберігання не на одному сервері, а копії бази даних є розповсюдженими по всіх учасниках мережі (нодах). Ноди синхронізуються між собою, тому, якщо хтось намагається змінити дані у своїй копії, система це виявляє та відхиляє зміну.

Основні принципи роботи блокчейну

Дані в блокчейні зберігаються у вигляді блоків, які формуються в ланцюг. Кожен блок містить:



Завдяки тому, що кожен блок містить хеш попереднього, зміна інформації в одному з блоків автоматично порушує цілісність всього ланцюга. Тому це дозволяє виявити несанкціоноване втручання в дані, оскільки будь-яка зміна в одному з блоків потребуватиме перерахунку хешів усіх наступних блоків, що неможливо без узгодження з більшістю учасників мережі. Саме ця особливість наділяє блокчейн такою властивістю як незламність.

Як тільки блок додається до блокчейну, змінити його неможливо без зміни всіх наступних блоків. Це гарантує:

- захист від шахрайства;
- прозорість;

- довіру між учасниками.

Крім того, завдяки використанню криптографічних алгоритмів дані залишаються зашифрованими і захищеними. Тобто особа, яка взаємодіє з іншою через технологію блокчейн, не знає, з ким саме вона має справу.



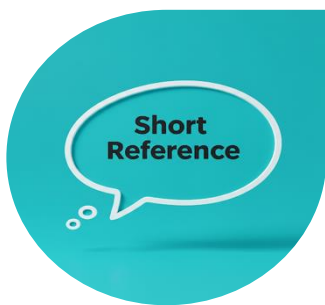
Або чому блокчейн вважається незламним?

1. **Хеш-функції:** Кожен блок містить унікальний хеш, і якщо хтось змінить дані в одному блоці, то всі наступні хеші зміняться, роблячи зміну очевидною.

2. **Proof of Work (PoW):** В Bitcoin та інших криптовалютах використовується алгоритм консенсусу, що вимагає значних обчислювальних ресурсів для додавання нового блоку, що ускладнює атаку.

3. **Децентралізація:** Оскільки дані зберігаються у великій кількості вузлів, зламати всі одночасно неможливо.

4. **Атака 51%:** Теоретично, якщо хтось отримає контроль над більш ніж 50% потужностей мережі, він зможе змінювати блокчейн. Але в реальності це надзвичайно складно і дорого.



Що таке хеш?

Хеш (hash) – це унікальний цифровий відбиток (значення фіксованої довжини), який генерується на основі вхідних даних за допомогою спеціальної математичної функції, званої **хеш-функцією**. Хешування використовується для забезпечення **безпеки, ідентифікації та перевірки цілісності даних**.

Хеш-функція бере вхідні дані (текст, файл, транзакцію тощо) та обробляє їх, повертаючи рядок фіксованої довжини. Наприклад, використання алгоритму **SHA-256** для слова «Blockchain» дає такий результат:

```
625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
```


Якщо змінити хоча б одну літеру, наприклад «blockchain» (з малої букви), результат буде зовсім іншим:

ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1²¹

Цей ефект називається **ефект лавини**: навіть мінімальна зміна вхідних даних призводить до кардинальної зміни вихідного хешу.

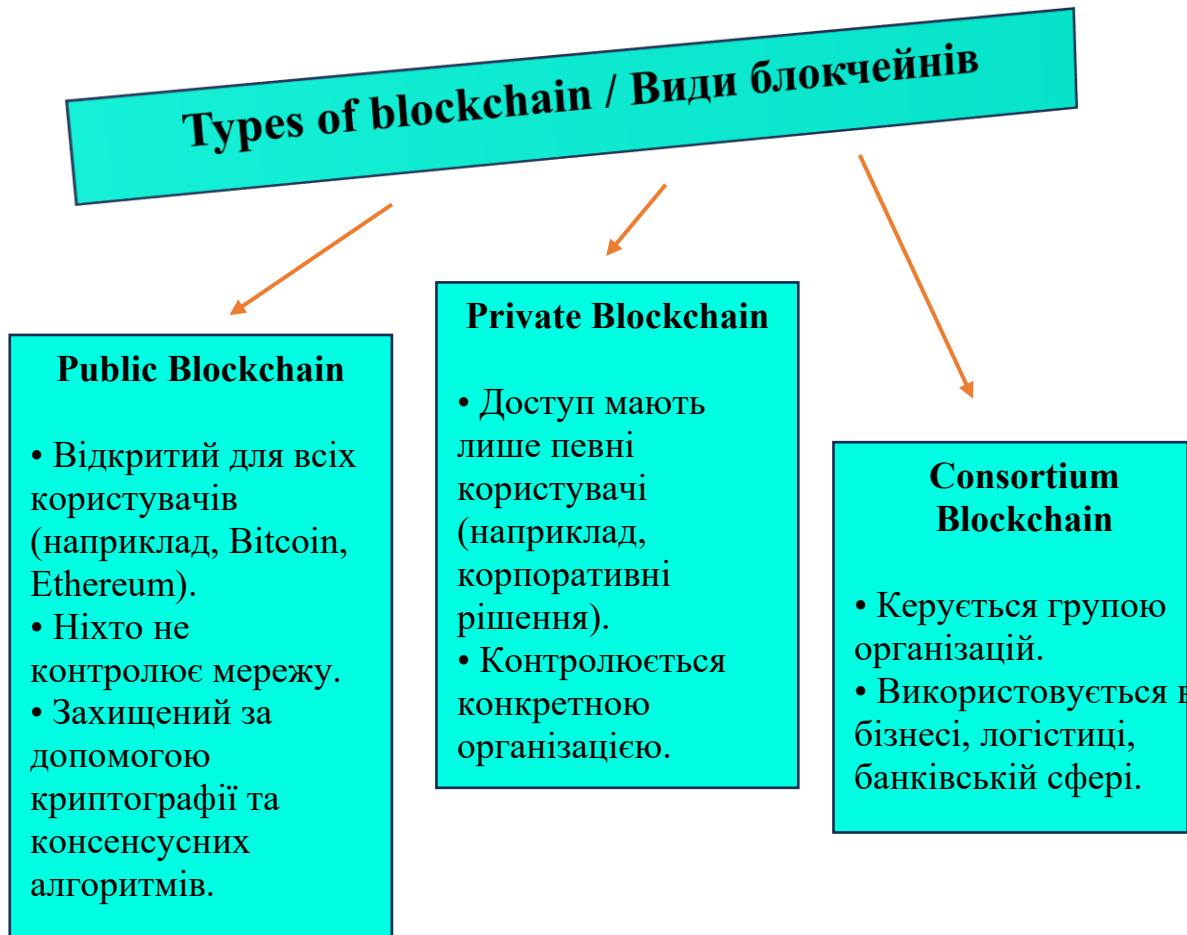
Сфери використання хешування:



2. Види та сфери застосування блокчейну

Хоча блокчейн часто асоціюють із криптовалютами, його можливості набагато ширші – він здатен змінити різні сфери, від фінансового сектору до державного управління.

²¹ Було зроблено на основі: SHA256 Generator Hash. KeyCDN. URL: <https://tools.keycdn.com/sha256-online-generator> (date of access: 17.03.2025).



Сфери застосування блокчейну:

1. **Фінанси.** Використовується у *криптовалютах, міжнародних платежах* (наприклад, блокчейн-платформи Ripple²² та Stellar²³ можна назвати вже навіть конкурентами міжнародній фінансовій мережі SWIFT, оскільки транзакції відбуваються за кілька секунд порівняно із SWIFTом – 1-3 дні, а також знімається низька комісія, адже операції виконуються без посередників), *банківських операціях* (Kinexys by JPMorgan²⁴, покращення доступності платежів, зменшення «конфлікту часових поясів», підвищення прозорості, швидкості врегулювання). **Виклики:** волатильність (коливання ціни фінансового активу), правове регулювання, енергоспоживання.

²² Global Payments & Financial Solutions for Businesses. *Ripple*. URL: <https://ripple.com> (date of access: 17.03.2025).

²³ Stellar. Blockchain Network for Smart Contracts, DeFi, Payments & Asset Tokenization. URL: <https://stellar.org> (date of access: 17.03.2025).

²⁴ Kinexys - Bank-Led Blockchain Solutions. *Kinexys by J.P. Morgan*. URL: <https://www.jpmorgan.com/kinexys/index> (date of access: 17.03.2025).

2. **Смарт-контракти.** Автоматичне виконання угод без посередників (Ethereum, Solana, Cardano). **Обмеження:** юридична визнаність, складність зміни умов контракту.

3. **Логістика.** Відстеження товарів та боротьба з підробками (IBM Food Trust²⁵, VeChain²⁶). **Виклики:** висока вартість впровадження, необхідність інтеграції з іншими системами.

4. **Голосування.** Електронні вибори з підвищеною прозорістю (i-Voting в Естонії²⁷ – використовують деякі принципи блокчейну, Voatz у США²⁸). **Обмеження:** безпека, довіра суспільства.

5. **Цифрова ідентифікація.** Використання для децентралізованих ідентифікаційних систем (Microsoft ION, генерує децентралізований цифровий ідентифікатор, який можна використовувати для входу/реєстрації на сайтах, підпису документів або доказу своєї особи).

Естонія використовує KSI Blockchain для захисту своїх державних реєстрів та перевірки змін у даних. Це означає, що записи про діяльність e-Residents (наприклад, реєстрація компаній) можуть бути перевірені за допомогою блокчейну. Також внаслідок використання естонськими урядовими мережами блокчейну KSI, інформація не може бути переписана ніким, а справжність електронних даних може бути математично доведена. Це означає, що ніхто - ні хакери, ні системні адміністратори, ні навіть сам уряд - не можуть маніпулювати даними і уникнути покарання²⁹. **Виклики:** необхідність державної підтримки.

Чим ION відрізняється від традиційних систем?

◆ Microsoft ION	◆ Google/Facebook Login
Децентралізована система	Централізована система

²⁵ Blockchain 101 by IBM Food Trust - Part 1: What is Blockchain? URL: https://mediacenter.ibm.com/id/1_5pyaubrs (date of access: 17.03.2025).

²⁶ VeChain - Web3 for Better: Sustainable Blockchain Solutions. URL: <https://vechain.org> (date of access: 17.03.2025).

²⁷ e-Democracy & open data - e-Estonia. URL: <https://e-estonia.com/solutions/e-governance/e-democracy/> (date of access: 17.03.2025).

²⁸ Voatz secure and convenient voting anywhere. URL: <https://voatz.com> (date of access: 17.03.2025).

²⁹ KSI blockchain - e-Estonia. URL: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/> (date of access: 17.03.2025).

Тільки користувач контролює ідентифікацію	Компанії контролюють акаунти
Дані не зберігаються на серверах компанії	Дані збираються та аналізуються
Не потребує паролів	Використовує традиційні паролі або 2FA (двофакторна авторизація)
Працює на блокчейні Bitcoin	Працює через корпоративні сервери

6. Нерухомість. Реєстрація власності (Propy³⁰, Mattereum³¹). **Обмеження:** юридичне регулювання, потреба у держреєстрах.

7. Медицина. Блокчейн використовують у медичній логістиці для відстеження ланцюга постачання медикаментів, що, у свою чергу, запобігає отриманню підроблених ліків, оскільки кожна партія має блокчейн-ідентифікацію (Pfizer³², Merck³³).

Загалом, використання блокчейну у медицині має великий потенціал, однак через високу конфіденційність та зарегульованість у сфері медичних даних, його складно реалізувати. Наприклад, були такі експериментальні проєкти як IBM Watson Health, MedRec (MIT), які мали забезпечити повний контроль пацієнтів над своїми медичними даними та швидкий доступ до них відповідних лікарів. Хоча нині ці проєкти не функціонують, однак наукові дослідження у цій сфері тривають.

Виклики: високі витрати, зарегульованість медичної сфери.

8. Освіта. Деякі університети пропонують випускникам, поряд з фізичним отриманням диплому, можливість отримати цифровий диплом на основі технології блокчейн, що унеможлиблює його підробку (Massachusetts Institute of Technology³⁴, University of Nicosia³⁵).

³⁰ Propy. 24/7 Real Estate Closings Powered by Tech. URL: <https://propy.com/home/> (date of access: 17.03.2025).

³¹ Mattereum. URL: <https://mattereum.com> (date of access: 17.03.2025).

³² How Does Pfizer Use Blockchain? – Exploring the Future of Emerging Technologies, Digital Economy, Data Security, and HealthTech. URL: <https://disruptionhub.com/how-does-pfizer-use-blockchain/> (date of access: 17.03.2025).

³³ Blockchain: a new security check for medicines. URL: <https://www.merckgroup.com/en/research/science-space/envisioning-tomorrow/smarter-connected-world/blockchain.html> (дата звернення: 17.03.2025).

³⁴ Digital diplomas. MIT Registrar. URL: <https://registrar.mit.edu/transcripts-records/diplomas/digital-diplomas> (date of access: 17.03.2025).

³⁵ Blockchain-based certifications - University of Nicosia. *University of Nicosia - The largest university in Cyprus*. URL: <https://www.unic.ac.cy/iff/research/blockchain-crypto-assets/blockchain-based-certifications/> (date of access: 17.03.2025).

Обмеження: висока вартість впровадження, юридична та нормативна невизначеність.

Потенціал блокчейну ще вивчається, тому не виключено, що сфери його застосування розширюватимуться у майбутньому.

3. Право і блокчейн-технології



Варто відзначити, що технологія блокчейн розвивається значно швидше, ніж правове регулювання відповідних правовідносин. Це є цілком логічним, дже право зазвичай реагує на появу нових суспільних відносин, а не випереджає їх. Водночас рівень правового регулювання у різних країнах суттєво відрізняється, що зумовлено як складністю ідентифікації окремих цифрових об'єктів, так і різними підходами до регулювання цієї сфери.

Ключові виклики для законодавчих органів:

у сфері регулювання блокчейн-технологій

Визначення правового статусу блокчейн-реєстрів та криптовалют.	У ЄС, наприклад, у 2023 році прийняли Регламент MiCA (Markets in Crypto-Assets Regulation) ³⁶ , що встановлює єдині правила для крипторинку.
Регулювання криптобірж, токенів.	
Оподаткування транзакцій у блокчейні.	
Дотримання вимог боротьби з відмиванням грошей (AML) та фінансуванням тероризму (CFT).	

³⁶ Regulation - 2023/1114 - EN - EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng> (date of access: 17.03.2025).

Захист прав інвесторів.	
у сфері регулювання смарт-контрактів	
Юридична сила (наприклад, чи можуть вони прирівнюватися до традиційних контрактів?).	Деякі країни, такі як США ³⁷ та Велика Британія ³⁸ , визнали смарт-контракти юридично обов'язковими в певних випадках.
Регулювання та відповідальність у разі помилок у коді.	
Співвідношення з традиційними правовими нормами про договірне право.	
у сфері інтелектуальної власності	
Визнання фіксації авторського права (реєстрація творів, патентів, торгових марок) за допомогою технології блокчейн.	У деяких юрисдикціях (Бельгія, Норвегія, Іспанія) NFT вже визнаються як докази володіння, тоді як в інших правові рамки ще розробляються ³⁹ .
Захист цифрового контенту через NFT (невзаємозамінні токени), які підтверджують власність на цифрові активи. Однак чи є NFT достатнім доказом володіння активом, і як врегульовуються спори?	
Контроль за використанням ліцензій.	
інші питання	

³⁷ USA: Smart Contracts Definition and Legality. *GitHub Pages*. URL: <https://neo-project.github.io/global-blockchain-compliance-hub//united-states-of-america/USA-smart-contracts.html> (date of access: 17.03.2025).

³⁸ Smart Legal Contracts. URL: https://webarchive.nationalarchives.gov.uk/ukgwa/20250109110910mp_/https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2021/11/6.7776_LC_Smart_Legal_Contract_s_2021_Final.pdf (date of access: 17.03.2025).

³⁹ Цифрові активи та ПДВ: робочий документ щодо оподаткування NFT. URL: https://biz.ligazakon.net/analytics/225505_tsifrov-aktivi-ta-pdv-robochiy-dokument-shchodo-opodatkovannya-nft (дата звернення: 17.03.2025).

Визначення сумісності децентралізованих ідентифікаційних систем заснованих на блокчейні з національним законодавством про ідентифікацію.

Відповідно до **GDPR** у ЄС (закон про захист персональних даних) передбачено «право на забуття» (видалення даних), але блокчейн за своєю природою не дозволяє редагувати або видаляти інформацію.

Це лише примірний перелік питань, які потребують вирішення на правовому рівні, де-факто, він набагато ширший. Але навіть такий перелік яскраво демонструє зв'язок права з використанням блокчейн-технологій. Більшість з цих питань ще є відкритими для багатьох країн світу, у тому числі і для України, що, своєю чергою, передбачає як кропітку роботу у регуляції таких правовідносин (а значить і потребу у відповідних дослідженнях), так і потенційно відкрити нішу на юридичному ринку праці, яка виходить за межі класичної юридичної науки.

4. Досвід України щодо впровадження блокчейн-технологій



EXPERIENCE OF UKRAINE

В Україні досвід застосування технології блокчейн на державному рівні розпочався ще у 2017 році. Першим зазнало такої технологічної трансформації державне підприємство «СЕТАМ» - система електронних торгів арештованим майном. Перехід на блокчейн зайняв 3

місяці, що дозволило повністю ліквідувати будь-які можливості для маніпулювання даними під час здійснення аукціонів⁴⁰. Надихнувшись позитивним досвідом ДП «Сетам», Міністерство аграрної політики та продовольства України також

⁴⁰ СЕТАМ став першим у світі аукціоном на blockchain та змінив назву на OPENMARKET. URL: <https://setam.gov.ua/article/setam-stav-pershim-u-sviti-auktsionom-na-blockchain-ta-zminiv-nazvu-na-openmarket> (дата звернення: 17.03.2025).

вирішило запровадити блокчейн у діяльності Державного земельного кадастру, щоб унеможливити підробку реєстраційних даних про право власності на земельну ділянку⁴¹. Однак, в силу різних об'єктивних причин, у тому числі технологічних та статусу інформації, яка міститься в Держземкадастрі, досягти поставленої мети так і не вдалося⁴².

Водночас на приватно-правовому рівні, у зв'язку з розвитком криптовалютного ринку у світі, використання технології блокчейн серед населення України також активно набирало обертів. Тому на державному рівні неодноразово піднімалося питання щодо регулювання відповідних правовідносин, робилися запити до відповідних міністерств щодо тлумачення поняття «криптовалюта», до Верховної Ради вносилися відповідні законопроекти, тощо. Станом на сьогодні (квітень 2025 р.) в Україні на нормативно-правовому рівні є роз'яснення Національного Банку України від 10 листопада 2014 р. щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin⁴³, згідно з яким криптовалюта вважається грошовим сурогатом.

Також у 2022 році був прийнятий Закон України «Про віртуальні активи»⁴⁴, який мав врегулювати правовідносини, що виникають у зв'язку з оборотом віртуальних активів, визначав права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів. Однак він так і **НЕ** набрав чинності.

Детальні причини цього описані в статті [Форсюк В. «Чому в Україні так і не запрацював Закон України "Про віртуальні активи"»](#)⁴⁵, з якою корисно буде ознайомитись за наданим гіперпосиланням.

⁴¹ Державний земельний кадастр перейшов на технологію Blockchain. URL: <https://minagro.gov.ua/news/derzhavniy-zemelniy-kadastr-pereyshov-na-tekhnologiyu-blockchain> (дата звернення: 17.03.2025).

⁴² Мартин А. Blockchain-кадастр, як Держгеокадастр народив мишу! URL: <https://agropolit.com/blog/271-blockchain-kadastr-yak-derjgeokadastr-narodiv-mishu> (дата звернення: 17.03.2025).

⁴³ Роз'яснення щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin. Національний Банк України від 10.11.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0435500-14#Text> (дата звернення: 17.03.2025).

⁴⁴ Про віртуальні активи. Закон України від 17.02.2022 № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20?find=1&text=блокч#Text> (дата звернення: 17.03.2025).

⁴⁵ Форсюк В. Чому в Україні так і не запрацював Закон України «Про віртуальні активи». URL: <https://rates.fm/ua-uk/expert-opinion/chomu-v-ukrayini-tak-i-ne-zapracyuvav-zakon-ukrayini-pro-virtualni-aktivi/> (дата звернення: 17.03.2025).

Однак, цілком імовірним наслідком прийняття цього Закону стало внесення змін до Цивільного кодексу України шляхом його доповнення статтею 179¹, відповідно до якої з'явилося нове поняття «цифрової речі».

Цивільний кодекс України

Стаття 179-1. Поняття цифрової речі

1. Цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність.

Цифровою річчю є віртуальні активи, цифровий контент та інші блага, щодо яких застосовуються положення частини першої цієї статті.

2. Особливості правового режиму цифрових речей визначаються законом. До цифрових речей застосовуються положення цього Кодексу про речі, якщо інше не встановлено цим Кодексом, законом або не впливає із сутності цифрової речі.

Окрім цього в Законі України «Про запобігання корупції» зазначено обов'язок суб'єктів декларування вказувати відомості про криптовалюту (п. 6 ч. 1 ст. 46 Закону)⁴⁶. А Національне агенство з питань запобігання корупції надало роз'яснення, що криптовалюту потрібно відображати у розділі нематеріальних активів при декларуванні доходів та майна суб'єктами декларування⁴⁷.

Отже, наразі в Україні правовідносини у сфері віртуальних активів врегульовано лише вкрай поверхово та фрагментарно. Однак, думається, що після завершення війни дані питання будуть врегульовані в недалекому майбутньому, зважаючи на активні попередні спроби.

Щодо застосування технології блокчейн на державному рівні, то ймовірно, попри певні труднощі та специфіку його функціонування, сфера його використання в подальшому також розширюватиметься.

Резюмуючи, потрібно відзначити, що блокчейн вже змінює правові системи країн, змушуючи держави адаптувати законодавство. Тому елементарне

⁴⁶ Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII. URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата звернення: 17.03.2025).

⁴⁷ Нематеріальні активи. URL: <https://wiki.nazk.gov.ua/category/deklaruvannya/hii-nematerialni-aktyvy/> (дата звернення: 17.03.2025).

розуміння цих технологій буде лише перевагою для майбутнього юриста. А більш просунутим у цій сфері доведеться й, можливо, віднаходити баланс між незмінністю записів та правом на виправлення/захист даних, встановлювати регулювання криптоактивів, визначати юридичну природу смарт-контрактів тощо.



ПЕРЕВІРКА ЗНАНЬ

Прочитайте питання, дайте відповіді та знайдіть відповідні слова у сітці, зафарбувавши їх кольором. Слова можуть бути розташовані у таких напрямках:



Word Search

1. What is the name of the first cryptocurrency that used blockchain technology?
2. What is the term for a block's unique digital fingerprint?
3. What do we call a digital agreement that executes automatically?
4. What is the full name of the anonymous creator of Bitcoin?
5. What type of blockchain is accessible only to selected users?
6. What is the opposite of a private blockchain, open to everyone?
7. What term refers to a group of organizations managing a shared blockchain?
8. What digital technology did Nakamoto propose in his 2008 paper?
9. What was the first application of blockchain technology?
10. What abbreviation stands for the EU regulation on personal data protection?

P	W	P	E	T	X	D	X	N	D	S	M	A	L	Z
O	N	R	B	D	O	R	T	S	K	U	G	M	C	D
J	K	I	I	X	H	M	E	E	D	F	P	J	K	S
U	V	V	T	A	N	A	C	S	F	Z	U	Z	X	U
V	B	A	C	D	X	M	S	W	J	F	B	I	Y	V
P	I	T	O	B	C	K	Y	H	D	O	L	C	J	D
Y	U	E	I	U	M	J	Q	B	H	O	I	A	X	B
L	U	Q	N	D	V	E	L	Y	R	B	C	H	H	A
S	A	T	O	S	H	I	N	A	K	A	M	O	T	O
D	H	M	U	I	T	R	O	S	N	O	C	B	W	G
S	M	A	R	T	C	O	N	T	R	A	C	T	G	I
M	V	K	I	L	N	I	A	H	C	K	C	O	L	B
E	G	H	C	B	C	L	T	T	H	V	Q	W	P	P
D	X	I	T	H	H	A	L	H	S	Z	G	D	P	R
C	R	Y	P	T	O	C	U	R	R	E	N	C	Y	T

ЗАВДАННЯ



1. Debate: «Will Blockchain Replace Notaries?»

Підготуйте аргументи для проведення дебатів щодо того, чи зможе блокчейн замінити традиційну систему нотаріату.



2. Discussion «Blockchain and the State: To Regulate or Not?»

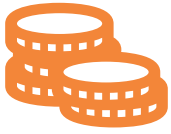
Підготуйте коротку позиційну записку (policy paper) з пропозиціями для законодавчого регулювання про те, чи потрібне державне регулювання блокчейну, чи він має залишатися децентралізованим.



3. Teamwork «Creating Infographics»

Підготуйте інфографіку, що пояснює, наприклад, юридичні ризики блокчейну (конфіденційність, шахрайство, незворотність

транзакцій тощо); відповідність блокчейна нормам міжнародного права; можливість використання блокчейну як доказ у суді.



4. Loss of Crypto Inheritance

Адвокатка отримала запит від родичів померлого підприємця, який володів криптовалютою на суму близько \$2 млн. Виявилося, що приватні ключі до гаманця були збережені у приватному цифровому нотатнику, до якого немає доступу. У заповіті згадка про криптовалюту відсутня.

Questions:

1. *Як кваліфікується криптовалюта у спадковому праві України? Чи це майно?*
2. *Які способи доведення права спадкоємців можуть бути прийнятні?*
3. *Запропонуйте модель регулювання «криптоспащини», яка забезпечить баланс між безпекою та доступністю.*

Розділ IV ТОКЕНИ

TOKENS

1. Етимологія і зміст поняття „токен“

Коли мова йде про блокчейн, токени – одна з найбільш обговорюваних тем. Токени – це об’єкти, які передаються в блокчейні. Токени обмінюються на торгових майданчиках. Токени володіють різними функціональними можливостями, можуть використовуватися для платежів, послуг і як цінні папери. Токени можуть представляти право власності на земельні ділянки або інші реальні активи, так звані «Real World Assets». Токени навіть можуть бути пов’язані з мистецтвом. То що ж таке токени насправді?

Поняття «токен» у його сучасному вживанні походить з англійської мови. Його етимологія веде до давньоанглійського «*tācen*» та ще глибше – до протогерманського «*taikna*»⁴⁸. Уже в ті часи це слово означало щось на кшталт «знаку, символу або доказу», отже, «токен» слугував позначенням чогось іншого. І донині в англійській мові слово «*token*» означає символ чогось.

Особливо виразним є приклад із платіжними засобами, номінальна вартість яких перевищує їхню внутрішню (матеріальну) вартість, вони позначаються як *Token Money*, тобто як гроші, які лише репрезентують грошову цінність⁴⁹. Сучасні паперові гроші є майже виключно «*Token Money*», банкноти являють собою набагато більшу цінність, ніж папір, на якому вони надруковані, і навіть монети більше не наближаються до номіналу. Точно так само токени світу блокчейну є «репрезентацією» чого-небудь. Токени представляють собою у цифровому світі блокчейна об’єкти або функції, які лежать в їхній основі, і таким чином стають (цифровими) знаками.

⁴⁸ Origin and history of *token*. URL: <https://www.etymonline.com/word/token> (дата звернення: 23.04.2025); глибше про етимологію терміну «токен» *Meier*; в: *Meier* (ред.), *MiCAR-Handbuch*, 2025, гл. 2 п. 20 і наст.

⁴⁹ *Token money*. URL: https://dictionary.cambridge.org/de/worterbuch/englisch/token-money#google_vignette (дата звернення: 23.04.2025); див. детальну аргументацію *Milne*, чому блокчейн-токени можуть бути зрозумілі лише за аналогією з токен-грошима, але насправді такими не є, *Milne*, *Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money*, *Journal of Money, Credit and Banking* 56 (2024), 1919.

Давайте докладніше розглянемо, якими функціями та об'єктами можуть бути представлені токени і як ця репрезентація виглядає на технічному рівні. Перш ніж глибше зануритися в токени в їхньому вузькому розумінні, потрібно провести розмежування між поняттями «токени» та «криптовалюта» (cryptocurrency).

У загальній дискусії не завжди стає зрозумілою різниця між ними. Кожен блокчейн має власні одиниці, за допомогою яких усередині цього блокчейна проводяться транзакції. Хоча блокчейн за своєю сутністю є особливим типом розподіленої бази даних, він розроблений таким чином, щоб фіксувати та підтверджувати перекази між різними адресами у мережі. У підсумку, всі блокчейни містять власні внутрішньо передані одиниці (токени). Ця передана одиниця (токен у вигляді криптовалюти)



Валідація — це процес перевірки правильності транзакцій або створення нових блоків у блокчейні. У результаті валідації перевіряється, чи не є транзакція шахрайською, чи є достатньо коштів, чи підпис дійсний тощо. Після успішної валідації транзакція потрапляє до блоку, а блок — у блокчейн.

використовується в межах блокчейну як платіжний засіб. Вони потрібні, наприклад, для оплати комісій або як винагорода валідаторам, які здійснюють валідацію транзакцій у мережі.

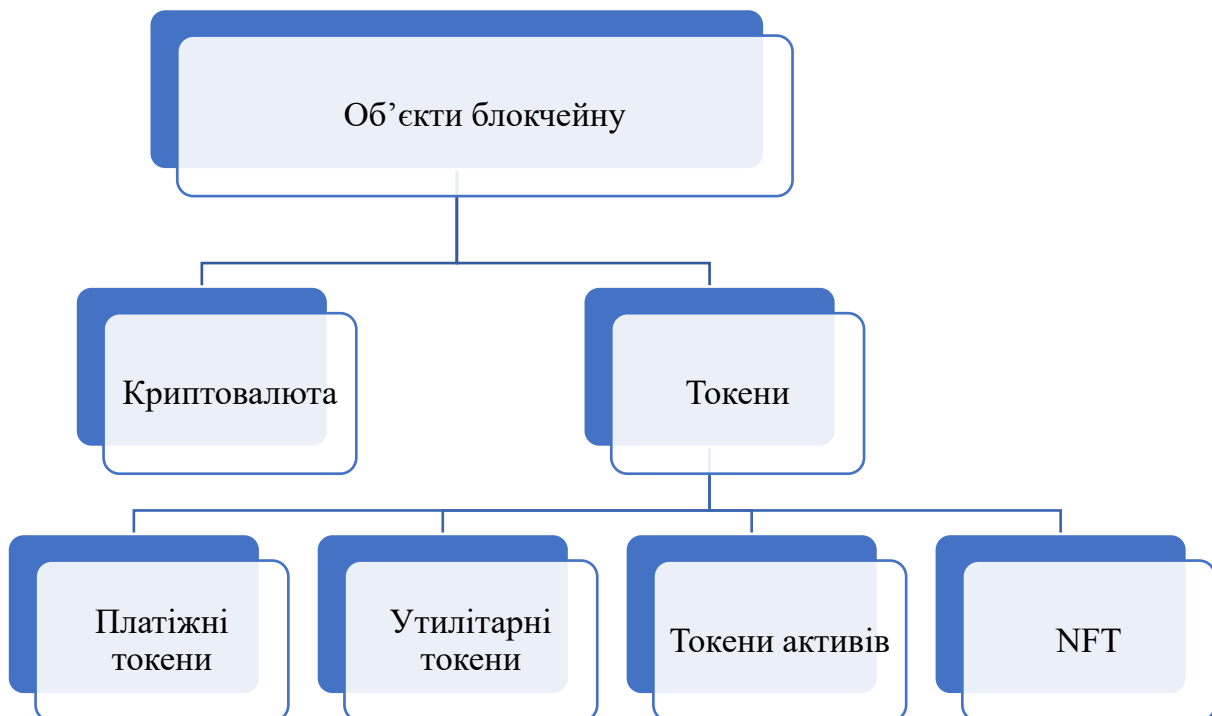
Платіж здійснюється у внутрішній «валюті» блокчейна, тому ці одиниці називають «криптовалютою». Так, Bitcoin-блокчейн використовує «Bitcoin» (BTC), Ethereum-блокчейн — «Ether» (ETH), а Solana-блокчейн — «Solana» (SOL) як відповідну внутрішню валюту своєї блокчейн-екосистеми. Ці криптовалюти суттєво відрізняються за своїм виникненням і застосуванням від «токенів», які будуть розглянуті детальніше пізніше. Криптовалюта виникає безпосередньо на наявному блокчейні, який визначає її правила⁵⁰. Тому криптовалюта — це підвид токенів,

⁵⁰ Хто хоче дізнатися, як саме працює, може ознайомитися з книгою Antonopoulos, Mastering Bitcoin, 2017, гл. 2, для біткойна, і з Antonopoulos/Wood, Mastering Ethereum, 2019, для ефіру.

головною метою якої є здійснення платіжних функцій у межах або поза межами блокчейн-системи. Токени виникають, навпаки, через смарт-контракти, які (залежно від блокчейну) може створити кожен користувач. Це відкриває не лише безмежну кількість можливих токенів, але й також необмежену кількість можливих токен-функцій, які ми розглянемо у наступному розділі.

2. Типологія токенів: функціональні види та техніко-програмна база

Тепер ми переходимо до основної теми цього розділу: до токенів. Ми вже встановили, що токени є цифровим відображенням об'єктів або функціями. Але що являють собою ці об'єкти та функції і як це виглядає технічно? Давайте розглянемо це докладніше. Нижче у схемі візуалізовано співвідношення токенів та криптовалюти, а також основні види токенів.



Класично токени поділяються на чотири типи: «платіжні токени» (Payment Tokens), «утилітарні токени» (Utility Tokens), широкую категорію «токени активів»

(Asset Tokens) і так звані «унікальні або невзаємозамінні токени» (Non-fungible Tokens) або коротко «NFT». Попри відмінності у функціональних властивостях і технічних характеристиках різних типів токенів, їхній процес виникнення має спільну основу. На початковому етапі розробник створює програмний код так званого «смарт-контракту» (Smart Contract), у якому визначає функціонал токена, порядок його придбання та передавання, а також можливі права, що з ним пов'язані. Після того як розробник запрограмував смарт-контракт, він запускає його в блокчейні і таким чином вводить у дію протокол токена.



Смарт-контракти - це комп'ютерні програми, які керують протоколами на блокчейні. Іншими словами - це програмний код, який реалізує принцип умовної логіки типу «якщо X — тоді Y». Основною умовою виконання такого контракту може бути, наприклад: «якщо 4 ЕТН перераховано на адресу А, тоді 40 А-токенів надсилаються на адресу відправника».

Смарт-контракти функціонують як спеціалізований механізм обліку, подібний до бухгалтерської книги, що оновлюється автоматично згідно із запрограмованими правилами. У системах, які базуються на балансовій моделі, зокрема в мережі Ethereum, смарт-контракт відстежує баланси та трансакції всіх *public address*, які взаємодіють із відповідними токенами. Актуальний стан цього обліку фіксується безпосередньо в блокчейні.

Кожен смарт-контракт має унікальну адресу в мережі блокчейну, яка функціонує аналогічно до *public address* звичайного користувача. Для взаємодії з ним достатньо ініціювати трансакцію на відповідну адресу. Смарт-контракт, як і будь-яка інша адреса, може мати власний баланс та здатен автоматично ініціювати трансакції на основі закладених у ньому умов виконання. На відміну від звичайних адрес, смарт-контракт не контролюється фізичною особою; його логіка повністю визначається закладеним програмним кодом [с.39]⁵¹. Це також означає, що будь-яка взаємодія з таким контрактом є незворотною після її підтвердження в блокчейні.

Тепер розглянемо детальніше кожен із типів токенів.

⁵¹ Antonopoulos, A. M., Wood, G. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol: O'Reilly Media, 2019. 385 с. 39.

2.1. Платіжні токени

Платіжні токени - це такі токени, які мають слугувати альтернативним засобом платежу⁵². В даному випадку зазвичай мова йде про «взаємозамінні» («fungible») токени. Взаємозамінність у цьому контексті означає, що кожен токен у своєму виконанні ідентичний, і тому токени взаємозамінні - іншими словами: для користувача не має значення, який конкретно токен він отримує від смарт-контракту.

У базовій формі платіжні токени налаштовані доволі просто: відповідні смарт-контракти передбачають, як (за яких умов) випускаються нові платіжні токени, чи існує максимальна кількість токенів і за яких умов токени можуть передаватися від однієї особи до іншої. Такі токени зазвичай не мають фіксованої ціни по відношенню до інших токенів або офіційних валют, тож їхня ціна визначається виключно попитом і пропозицією на ринку. У результаті спостерігаються подекуди значні цінові коливання різних платіжних токенів на криптовалютних торговельних платформах⁵³. Простота програмування таких токенів також спричиняє їх масову появу: станом на квітень 2025 року на ринку налічується понад 10 000 активних платіжних токенів⁵⁴. Цю тенденцію ще більше посилюють платформи, які беруть на себе весь процес програмування таких токенів для користувача, тож останньому фактично достатньо лише обрати назву⁵⁵.

Але є й інші токени, які також мають слугувати платіжним засобом, ціна яких прив'язана до певної еталонної вартості, так звані стейблкоїни «stablecoin». Частково stablecoin розглядаються як окрема категорія, частково ж вони належать до платіжних токенів. У будь-якому разі, stablecoin – це набагато складніші

⁵² BaFin. Guidance Notice. Second advisory letter on prospectus and authorization requirements in connection with the issuance of crypto tokens 22.11.2019. URL: <https://www.bafin.de/ref/19593866> (date of access: 30.04.2025).

⁵³ Це також призводить до критики таких платіжних токенів, оскільки цінності з високою волатильністю в принципі не підходять як засіб платежу.

⁵⁴ Duarte Fabio. How Many Cryptocurrencies are There in 2025? URL: <https://explodingtopics.com/blog/number-of-cryptocurrencies> (date of access: 30.04.2025).

⁵⁵ Найвідоміша платформа наразі - це «pump.fun», яка дає змогу створювати так звані «мемкойни» всього за кілька кліків.

токени, ніж класичні платіжні токени, оскільки *stablecoin* повинні мати механізм для підтримання фіксованого співвідношення між токеном і еталонною вартістю⁵⁶.

Створення класичних платіжних tokenів жорстко стандартизовано, оскільки з технічного погляду йдеться про відносно прості смарт-контракти. Найпоширенішим технічним стандартом є так званий стандарт **ERC-20**, на основі якого функціонує велика кількість взаємозамінних tokenів, зокрема платіжних.



З метою забезпечення того, щоб смарт-контракти в межах одного блокчейну могли безперешкодно взаємодіяти між собою (тобто були **інтероперабельними**) та могли будуватися один на одному (тобто були **композиційно сумісними**), розробляються стандарти, відповідно до яких здійснюється програмування смарт-контрактів. Найвідомішими є стандарти, створені для екосистеми

Ethereum, які також справляють вплив на інші блокчейн-платформи.

У мережі Ethereum пропозиції щодо впровадження таких стандартів мають назву **EIP** (*Ethereum Improvement Proposals*), тоді як самі стандарти tokenів позначаються як **ERC** (*Ethereum Request for Comments*)⁵⁷. Розробники, які мають намір створити новий смарт-контракт, як правило, орієнтуються на зазначені стандарти з метою мінімізації витрат на розробку, а також для забезпечення інтероперабельності та композиційної сумісності рішень.

Попри домінуюче становище стандартів Ethereum, багато інших блокчейн-систем також розробляють власні стандарти, адаптовані до технічних і функціональних особливостей відповідної мережі.

Стандарт **ERC-20** визначає основні функції та складові частини взаємозамінних tokenів. До них належать: загальна кількість tokenів смарт-контракту, баланси всіх власників tokenів, спосіб передавання tokenів (тобто за

⁵⁶ Як це досягається, можна прочитати, наприклад, тут: Baughman G., Carapella F., Gerszten J., Mills D. The stable in stablecoins. FEDS Notes. December 16, 2022. URL: <https://www.federalreserve.gov/econres/notes/feds-notes/the-stable-in-stablecoins-20221216.html> (date of access: 23.04.2025).

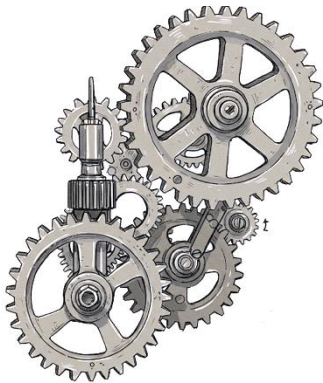
⁵⁷ Ethereum Development Standards. URL: <https://ethereum.org/en/developers/docs/standards/> (date of access: 30.04.2025).

яких умов токени можуть передаватися з однієї адреси на іншу), дозвіл третім особам переказувати токени (тобто механізм, за допомогою якого можна надати третій особі право розпорядження) та функція сповіщення про події у смарт-контракті (наприклад, про передання токена з однієї адреси на іншу), що слугує для інформування мережі про зміни⁵⁸.

2.2. Утилітарні токени

На відміну від платіжних токенів, утилітарні токени мають внутрішню функціональність, що виходить за рамки простої передачі від однієї особи до іншої.

У той час як платіжні токени служать переважно для передачі між людьми, утилітарні токени *втілюють право на послугу або продукт чи слугують засобом доступу до послуги або продукту*, який можна порівняти з квитком або ваучером⁵⁹.



Тому їх часто називають «Utility»-токенами (англ. «Utility» означає, серед іншого «корисність»), оскільки такі токени мають додаткові функції. Часто такі токени продаються в рамках «ICO» (англ. «Initial Coin Offerings» – первинний випуск монет). На момент їхнього продажу зазвичай ще не існують продукти та послуги, які вони втілюють, тому утилітарні токени слугують для фінансування розробки відповідного продукту. Власники утилітарних токенів спекулюють на тому, що їхні інвестиції в майбутньому окупляться доступом до цього продукту через свій утилітарний токен.

З технічного погляду утилітарні токени також ґрунтуються на стандарті ERC-20 або суміжних (аналогічних) стандартах. Додаткові функціональні можливості утилітарних токенів потім програмуються або в самому вихідному

⁵⁸ ERC-20 Token Standard. URL: <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> (date of access: 30.04.2025).

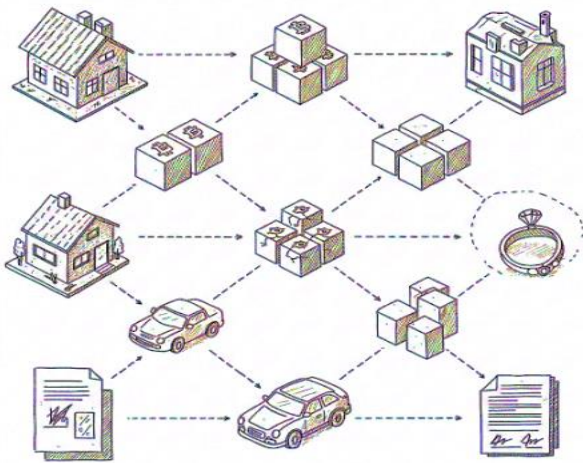
⁵⁹ BaFin. Guidance Notice. Second advisory letter on prospect and authorization requirements in connection with the issuance of crypto tokens. 2019. URL: <https://www.bafin.de/ref/19593866> (date of access: 30.04.2025).

смарт-контракті, або в інших смарт-контрактах. Наприклад, якщо утилітарний токен надає доступ до іншого продукту в межах того самого блокчейну, то в смарт-контракті цього продукту права доступу пов'язуються з емітованим утилітарним токеном.

До речі: це також ілюструє необхідну інтероперабельність і композиційну сумісність різних смарт-контрактів, яка була описана вище. Щоб смарт-контракт продукту міг безперешкодно звертатися до ERC-20 смарт-контракту утилітарного токена, останній має бути стандартизований. Тільки так інший смарт-контракт зможе викликати потрібні функції, наприклад, для перевірки балансу відповідного користувача, щоб переконатися, що в нього достатньо утилітарних токенів.

2.3. Токени активів, включаючи «security» - токени

Широке значення мають токени активів (Asset Tokens), які складають основу так званої «токенізації». «Токенізація» описує процес перенесення об'єктів, які перебувають за межами блокчейну, на блокчейн [с. 11]⁶⁰.

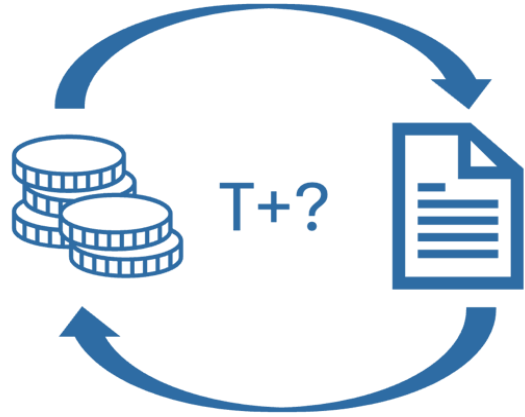


Тобто токенізація – це цифрове відображення «реальних» об'єктів. Це можуть бути фізичні об'єкти, наприклад, картини, земельні ділянки, золото тощо (так звані «Real-World-Assets» або коротко «RWA»).

Токени активів можуть також представляти собою нематеріальні цінності, наприклад, частки в компанії (зокрема, акції) або боргові зобов'язання (наприклад, облігації). Права, втілені в токенізованих активах, часто називають в англomовній літературі «Security Tokens». В індустрії очікується, що цілісна токенізація принесе широкий спектр переваг, які не обмежуються фінансовою

⁶⁰ Tokenise Europe 2025, Should Europe Develop into a Token Economy? URL: <https://bankenverband.de/en/digital-world/tokenise-europe-2025-new-initiative-shows-benefits-tokenisation> (date of access: 30.04.2025).

індустрією, а пов'язані з Internet of Things (IoT), безпілотним транспортом, великими даними (Big Data), іграми, метавсесвітом і багатьма іншими галузями. Загалом говорять про цифровізовану «Індустрію 4.0» [с. 11]⁶¹. Токени активів тим часом відіграють дедалі більшу роль, особливо у фінансовому секторі, можливо, навіть найбільшу [с. 13]⁶². Блокчейн пропонує тут значні переваги в процесі обробки транзакцій на фінансових ринках. Традиційно такі транзакції, як, наприклад, обмін акції на грошові кошти (причому розрахунок відбувається не одразу, а за принципом «платіж проти поставки»), є досить трудомісткими. Наразі в ЄС з моменту укладення контракту до розрахунків за угодою (тобто до моменту передання акцій покупцю та отримання грошей продавцем) проходить 2 дні (так званий «T+2»). ЄС наразі працює над тим, щоб скоротити цей період на «T+1»⁶³.



Для порівняння: Німецька компанія Siemens уже три роки проводить тести з випуску токенизованих активів на блокчейні. В останньому тесті у вересні 2024 року обробка транзакції тривала всього п'ять хвилин⁶⁴. Ефективність та економія витрат очевидні. Тому токени активів і необхідна для них інфраструктура розглядаються, розробляються і досліджуються з великим інтересом.

Як неважко здогадатися, технічна сторона токенів активів зазвичай є значно складнішою порівняно з іншими видами токенів. У той час як (юридичний) зв'язок між токеном і відповідним активом є не технічним, а саме правовим питанням, технічні вимоги до токенів активів є складнішими. Це зумовлено, зокрема, необхідністю особливого оформлення повноважень,

⁶¹ Tokenise Europe 2025, Should Europe Develop into a Token Economy? URL: <https://bankenverband.de/en/digital-world/tokenise-europe-2025-new-initiative-shows-benefits-tokenisation> (date of access: 30.04.2025).

⁶² The Tokenisation of Assets and Potential Implications for Financial Markets. *Report*. 27.03.2020. URL: <https://doi.org/10.1787/83493d34-en> (date of access: 30.04.2025).

⁶³ Castaldo, T+1 settlement. URL: https://finance.ec.europa.eu/news/t1-settlement-2025-02-14_en (date of access: 30.04.2025).

⁶⁴ Siemens AG. Siemens remains a pioneer – Another digital bond successfully issued on blockchain. 04 September 2024. URL: <https://press.siemens.com/global/en/pressrelease/siemens-remains-pioneer-another-digital-bond-successfully-issued-blockchain> (date of access: 30.04.2025).

урахуванням суворіших юридичних вимог або потребою у відображенні процесів фізичного світу в блокчейні. Попри те, що використання стандарту ERC-20 (або, альтернативно, ERC-721 для NFT — про це йтиметься далі) для токенів активів є технічно можливим і частково застосовується на практиці, з часом були розроблені інші стандарти, які дозволяють більш точно та детальне програмування токенів цього типу.

Для токенів, що представляють реальні активи (RWA-токенів), у блокчейні Ethereum було розроблено стандарт ERC-3643. Цей стандарт ґрунтується на загальному стандарті ERC-20, модифікуючи його таким чином, щоб забезпечити відповідність специфічним вимогам RWA-токенів. Насамперед йдеться про можливість інтеграції правил відповідності (compliance)⁶⁵. Зокрема, стандарт розроблений концептуально так, щоб токени могли належати виключно тим особам, які пройшли ідентифікацію відповідно до протоколу управління ідентифікацією. Це пояснюється тим, що національне законодавство в окремих юрисдикціях може вимагати таку ідентифікацію, наприклад, з метою протидії відмиванню коштів (AML).

Крім того, на основі реалізації вимог щодо відповідності (compliance) для токенізованих цінних паперів (security tokens) було розроблено низку спеціалізованих стандартів. Для security tokens також розглядається можливість застосування стандарту ERC-3643, однак і в цьому випадку управління ідентифікацією користувачів залишається суттєвою проблемою. У цьому контексті часто згадуються також стандарти ERC-1400 та ERC-1404, які дозволяють реалізовувати базові вимоги до функціонування security tokens⁶⁶. Проте багато таких токенів не дотримуються зазначених стандартів і програмуються індивідуально. Це часто зумовлено особливими (насамперед юридичними) вимогами, яких мають дотримуватися токенізовані цінні папери відповідно до конкретного нормативно-правового середовища. У будь-якому разі, при розробці таких токенів зазвичай приділяється увага тому, щоб вони були

⁶⁵ ERC-3643. URL: <https://eips.ethereum.org/EIPS/eip-3643> (date of access: 30.04.2025).

⁶⁶ Tangany. Ethereum ERC-standards and their business use-cases. 23. December 2020. URL: <https://tangany.com/blog/ethereum-erc-standards-and-their-business-use-cases> (date of access: 30.04.2025).

сумісні зі стандартом ERC-20, що забезпечує їхню інтеграцію та безперешкодне використання в екосистемі Ethereum.

2.4. Невзаємозамінні токени (NFT)

Відмінність «невзаємозамінних токенів» («non-fungible Token», NFT) від інших токенів уже закладена в їхній назві: вони не є взаємозамінними, тобто, не можуть бути замінені одне одним. Кожен з них є індивідуалізованим і використовується для унікальних об'єктів. Примітно, що право власності на унікальний об'єкт може бути представлено через токен. На основі NFT сформувався масштабний ринок цифрового мистецтва, оскільки NFT дають змогу ексклюзивно репрезентувати право власності на цифровий твір мистецтва. Водночас NFT використовуються і в багатьох інших сферах. В сфері відеоігор, наприклад, NFT можуть застосовуватися для представлення права власності на колекційні предмети (collectibles). Окрім того, згадані вище токени активів також частково реалізуються у формі NFT (найчастіше – як серії NFT), якщо виникає потреба відобразити право власності на конкретний фізичний об'єкт, наприклад, на нерухомість.

З технічного погляду такі NFT повинні мати можливість бути індивідуалізованими, що досягається завдяки використанню унікального ідентифікатора. У мережі Ethereum це реалізується через застосування стандарту ERC-721⁶⁷. Цей стандарт визначає, з одного боку, механізм індивідуалізації токенів за допомогою так званого TokenID (ідентифікаційного номера відповідного токена), який є унікальним у межах самого смарт-контракту. Його унікальність в усьому блокчейні забезпечується комбінацією TokenID та адреси смарт-контракту. З іншого боку, стандарт передбачає можливість збереження метаданих, що стосуються об'єкта, який репрезентується токеном. Наприклад, якщо йдеться про цифровий твір мистецтва, то в URI (Uniform Resource Identifier — стандартизована послідовність символів для ідентифікації інтернет-ресурсів;

⁶⁷ ERC-721: Non-Fungible Token Standard. URL: <https://eips.ethereum.org/EIPS/eip-721> (date of access: 30.04.2025); менш технічне пояснення можна знайти тут: <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/> (дата звернення: 30.04.2025).

до URI відноситься URL, тобто інтернет-адреса) міститься посилання на місце зберігання цього цифрового об'єкта. Такі твори часто зберігаються у децентралізованих мережах зберігання даних, наприклад у IPFS (InterPlanetary File System)⁶⁸. Крім того, стандарт ERC-721 також передбачає низку складових, аналогічних до стандарту ERC-20, зокрема можливість передавання токенів.



Приклади цифрових персонажів з NFT-колекції Bored Ape Yacht Club (BAYC)

На зображенні представлено приклади цифрових персонажів з NFT-колекції Bored Ape Yacht Club (BAYC). Це одна з найвідоміших і найдорожчих колекцій невзаємозамінних токенів (NFT) у світі, створена компанією Yuga Labs у 2021 році. Кожна мавпа є унікальним зображенням, створеним за допомогою автоматичного поєднання різних візуальних

елементів (фон, одяг, аксесуари, вираз обличчя тощо), і водночас — це токен у блокчейні Ethereum, що підтверджує право власності на цифровий об'єкт.

Попри гротескний, подекуди навіть примітивний візуальний стиль, зображення з колекції BAYC стали предметом ажіотажного попиту. Їхня популярність зумовлена не лише цифровою рідкісністю, а й символічною та соціальною цінністю. NFT-мавпи виконують функцію цифрової візитівки, ознаки належності до престижного онлайн-клубу, елемента бренду чи особистої ідентичності у віртуальному середовищі. Колекція набула статусу «елітної», її об'єкти купували й публічно демонстрували світові знаменитості: Снуп Догг, Емінім, Мадонна, Стів Аокі, Стеф Каррі та інші.

На піку популярності ціна одного NFT з колекції BAYC сягала від 200 000 до 400 000 доларів США, а деякі примірники продавались за понад 3 мільйони доларів (станом на 2024–2025 роки ціни значно впали, до \$30 000 – 40 000, що є наслідком загального падіння ринку NFT). Це створило прецедент, коли NFT почали сприймати не лише як цифрове мистецтво, а як спекулятивний фінансовий інструмент, аналог дорогих картин, антикваріату чи предметів розкоші.

Окрему юридичну вагу має той факт, що BAYC надає власникам NFT ліцензійні права на комерційне використання зображення, чим дозволяє створювати мерч, відкривати

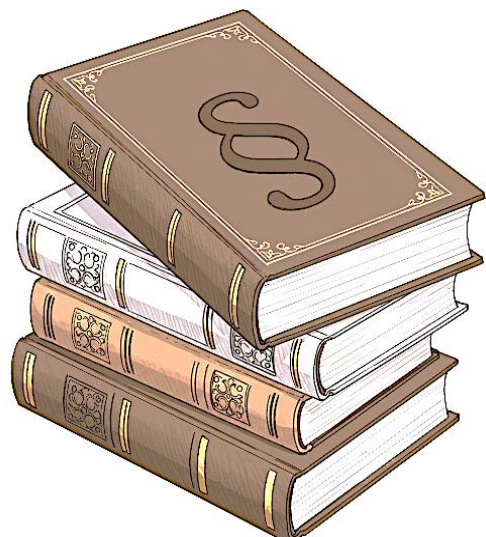
⁶⁸ Хто бажає дізнатися, що таке InterPlanetary File System (скорочено: IPFS) і як вона працює, може зробити це за посиланням: <https://docs.ipfs.tech/concepts/#learn-the-basics> (дата звернення: 23.04.2025).

заклади, видавати комікси тощо з використанням образу конкретної мавпи. Таким чином, NFT-мавпа стає не лише цифровим активом, а й об'єктом підприємницької діяльності.

Той факт, що поява блокчейну і токенів ставить глобальні правові системи перед викликами, особливо яскраво простежується в численній юридичній літературі та в триваючих дискусіях щодо законодавчих ініціатив по всьому світу. Правові системи суттєво відрізняються залежно від держави, а в окремих випадках – навіть у межах однієї держави (досить поглянути на США, чий федералізм породжує в підсумку 50 різних правових систем). На цьому тлі особливо цікаво спостерігати, що правові питання, пов'язані з токенами, які виникають, у різних правових системах багато в чому схожі. Тому міжнародні асоціації також активно долучаються до обговорення та пошуку відповідей на ключові юридичні питання, що виникають у зв'язку з розвитком токенизації⁶⁹.

3. Правові проблеми та виклики токенизації

У подальшій частині розділу буде розглянуто низку фундаментальних питань, покликаних окреслити коло ключових юридичних проблем, проте без претензії на остаточне їх вирішення. При цьому розмежування між різними типами токенів здійснюватиметься лише епізодично. Водночас відмінності у їх функціональному призначенні мають бути обов'язково враховані в рамках поглибленого юридичного аналізу.



⁶⁹ Особливу увагу слід приділити Принципам *UNIDROIT* з цифрових активів і приватного права, які вже вплинули на Єдиний торговельний кодекс США, а також розгляду феномена «токенів» такими організаціями, як *Financial Action Task Force (FATF)* і *Financial Stability Board (FSB)*.

3.1. Юридична природа токенів

Одним із великих досягнень токенів є технічна можливість забезпечити «цифрове володіння», тобто однозначне присвоєння цифрових об'єктів особою (або public address) і залишення їх під своїм контролем. Але чи відображає право це технічне досягнення?

Токени існують виключно в цифровій формі; по суті, вони є не чим іншим, як цифровою інформацією, що зберігається в базі даних. Коли користувач має токен у власному електронному гаманці (wallet), у нього виникає враження, що токен йому «належить» і що він може ним «розпоряджатися». Однак токен є нематеріальним: його не можна фізично відчутти, як автомобіль; він не є візуально сприйнятним, як будівля; його неможливо передати іншій особі з рук у руки, як, наприклад, банкноту. Отже, що таке токен з юридичного погляду — поза межами його існування як цифрової інформації?

Питання про правову природу токена породжує низку інших важливих правових проблем. Правова природа визначає характер володіння токеном, а отже — і правовий захист позиції власника токена, порядок передачі прав на токен, особливості укладення договорів, пов'язаних із токенами, можливість використання токенів як предмета застави, а також порядок їх реалізації у разі звернення стягнення на майно, і багато інших аспектів правового регулювання.

Відповіді на ці питання є складними та залежать від конкретної правової системи. Первинне, загальне розмежування зазвичай проводиться між двома основними глобальними правовими традиціями: common law (системою загального права) та civil law (континентальною (романо-германською) правовою системою)⁷⁰. У зв'язку з відсутністю кодифікації в системі common law,

⁷⁰ Common law характеризується тим, що формується насамперед судовою практикою. Судді виносять рішення в межах правової традиції, ґрунтуючись на попередніх судових рішеннях (precedent), а не на писаних законах. Система загального права діє насамперед у Великій Британії, США та в багатьох юрисдикціях, історично пов'язаних із Великою Британією, таких як, наприклад, Сінгапур. На противагу цьому стоїть civil law, яке ґрунтується на писаних законах. Правові питання не можуть вирішуватися на основі правової традиції, бо потребують попередньої кодифікації з боку законодавця. Суддя в цій системі не здійснює правотворчість, а займається тлумаченням і застосуванням закону. До країн civil law належать, наприклад, Німеччина та Україна. Вступ до цих двох правових традицій можна знайти, наприклад, у Dainow, *The Civil Law and the Common Law: Some Points of Comparison*, American Journal of Comparative Law 3 (1967), 419.

питання правової кваліфікації токенів у речово-правовому сенсі видається особливо гнучким. Попри те, що в різних юрисдикціях, які належать до традиції загального права, ведуться дискусії щодо конкретної правової природи токенів, здається, існує певний консенсус щодо того, що токени можуть визнаватися об'єктом власності особи та що з ними можуть бути пов'язані певні майнові права⁷¹. Натомість у системі *civil law* виникають певні труднощі. Для надання токенам статусу об'єкта права власності необхідне відповідне нормативне закріплення. У багатьох правових системах континентального права (хоча й не у всіх!) право власності традиційно пов'язане з фізичними об'єктами, тоді як токени існують виключно в цифровій формі. Вони не мають матеріальної субстанції, а отже, не розглядаються як об'єкти речового права в класичному розумінні. Хоча правові системи континентального типу загалом визнають майнові права на нематеріальні активи, така правова конструкція потребує чіткої кодифікації, яка у випадку з токенами в багатьох юрисдикціях досі відсутня.

Юридична природа токена набуває ще одного виміру, коли токен хочуть пов'язати з правом або вимогою, як це регулярно буває у випадку утилітарних токенів і токенів активів. Такий токен, званий також «зовнішнім» токеном (оскільки він пов'язаний із правом, яке перебуває за межами токена), функціонально являє собою свого роду цінний папір. Цінні папери характеризуються тим, що вони посвідчують право. Таке посвідчення призводить до того, що з переходом права на цінний папір переходять усі засвідчені ним права в сукупності; цінний папір і право поділяють одну й ту саму долю. Саме так і мають функціонувати зовнішні токени. Їх призначення полягає в тому, щоб зробити певне право на блокчейні (тобто в електронному вигляді) таким, що передається і використовується.

Питання про те, чи можуть токени бути цінними паперами не лише у функціональному, а й у юридичному розумінні, залежить від застосовного законодавства. З точки зору цивільного права, у багатьох правових системах для

⁷¹ Так, наприклад, в одній німецькій роботі, що порівнює сінгапурське і німецьке право, Bartylla/Meier, в: Omlor/Lübke (ред.), *Tokenized Finance*, 2025, стор. 153.

визнання активу цінним папером необхідне матеріальне посвідчення у формі фізичного сертифіката – іншими словами, цінний папір має бути саме «папером» у буквальному сенсі. Оскільки токени таким критерієм не відповідають, у відповідних юрисдикціях вони не можуть бути кваліфіковані як цінні папери в юридичному розумінні.

До 2021 року німецьке цивільне законодавство також передбачало обов'язкову наявність фізичного документа як умову для існування цінного папера, без можливості альтернативної форми посвідчення. Проте з прийняттям у 2021 році Закону про електронні цінні папери (*Gesetz über elektronische Wertpapiere, eWpG*) у Німеччині було створено правові підстави для електронної сек'юритизації цінних паперів, що відтоді дозволяє (за визначених умов) використання токенів як форми цінних паперів.

Хоча деякі юрисдикції й надалі не визнають електронну сек'юритизацію, інші країни вже давно це дозволяють. Наприклад, у США електронне посвідчення прав у формі безсертифікатних цінних паперів (*uncertificated securities*) визнається ще з 1977 року.

Якщо зовнішній токен не може бути юридично визнаний як цінний папір, то зв'язок між токеном і базовим правом виникає виключно на підставі договору. Оскільки зазвичай така договірна прив'язка є можливою, у разі виникнення конфлікту можуть виникнути суттєві юридичні проблеми. Наприклад, що станеться, якщо передача токена відбудеться відповідно до домовленості, але сам договір про передачу базового права містить юридичний дефект, який робить його недійсним? У такому разі токен передається, однак він є «порожнім», тобто не забезпечує передавання пов'язаного права вимоги, а відтак не виконує свого призначення. Таким чином, якщо токен не є цінним папером, договір тільки призводить до того, що токен і право за договором повинні *мати* однакову долю, однак це не обов'язково відбувається.

3.2. Юридичні невизначеності у сфері токенів: потреба в системному врегулюванні



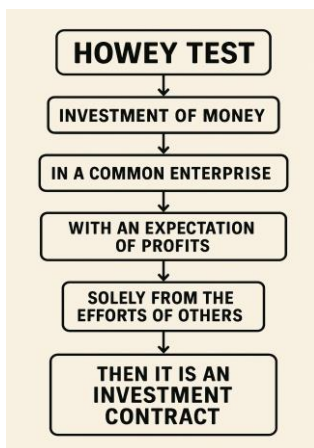
Законодавство про нагляд за фінансовими ринками визначає вимоги, яких мають дотримуватися учасники фінансового ринку. Таким чином, ідеться не про відносини між приватними особами, а про відносини між державою, яка реалізує свої інтереси (наприклад, забезпечення фінансової стабільності) та суб'єктами, які діють на фінансовому ринку. Поява токенів зумовила формування власних ринків, частина з яких перетинається з традиційним фінансовим ринком. У зв'язку з цим у різних країнах світу тривають дискусії щодо того, в якій мірі наглядове фінансове регулювання має поширюватися і на токени. З погляду фінансового регулювання, у цьому контексті постають два ключові питання: по-перше, як слід кваліфікувати самі токени, і, по-друге, як оцінювати послуги, пов'язані з токенами, відповідно до законодавства про нагляд. Ці два аспекти є взаємопов'язаними, оскільки регуляторна кваліфікація послуги залежить від того, до якого типу продукту вона відноситься.

Із моменту появи токенів на ринку в центрі дискусій опинилося питання про те, чи можна вважати токени «цінними паперами» або «фінансовими інструментами» в регуляторному сенсі. Термін «фінансовий інструмент» є узагальнюючим і вживається, зокрема, в законодавстві Європейського Союзу, тоді як «цінний папір» частіше застосовується до тих фінансових продуктів, які обертаються на ринку та репрезентують певні права й обов'язки сторін (наприклад, акції, облігації або деривативи).

Варто зазначити, що віднесення токена до категорії цінних паперів у цивільно-правовому розумінні не обов'язково означає його визнання як цінного папера або фінансового інструмента у контексті наглядового законодавства. Як зазначалося вище, в цивільному праві цінним папером є

інструмент, що сек'юритизує право, тоді як у регуляторному контексті цінним папером вважається лише продукт, що підпадає під дію законодавства про фінансові ринки. Так, наприклад, ваучер на отримання послуги, що надається компанією (скажімо, ваучер на доступ до хмарного сховища), може бути реалізований у формі токена й за певних умов визнаватися цінним папером згідно з цивільним правом конкретної юрисдикції. Проте це не робить такий ваучер фінансовим інструментом у регуляторному сенсі. До фінансових інструментів, які регулюються наглядовим законодавством, передусім належать акції, облігації або інші сек'юритизовані права, що обертаються на організованих фінансових ринках.

У світовому масштабі найбільша увага до цієї дискусії була зосереджена у США. Американський орган регулювання фінансових інструментів (*Securities Exchange Commission, SEC*) дійшов висновку, що переважна більшість токенів підпадає під термін «цінний папір» з погляду регулювання і, отже, підпадає під правила регулювання фінансового ринку. Ця точка зору ґрунтується на вимогах рішення Верховного суду (*Supreme Court*) від 1946 року (так званий «*Howey Test*»), яке дотепер вважається прецедентом для кваліфікації цінного паперу відповідно до



Елементи *Howey Test*

законодавства про нагляд за фінансовими ринками⁷². З іншого боку, індустрія часто не погоджувалася з цим, стверджуючи, що їхні токени не відповідають усім критеріям тесту *Howey Test*. Це призвело до численних судових розглядів між SEC та представниками галузі. Паралельно, хоча і менш публічно, відбувалася дискусія в ЄС. Німецький наглядовий орган («BaFin») опублікував 2019 року лист, у якому обговорювалася можливість віднесення токенів до категорії цінних паперів⁷³.

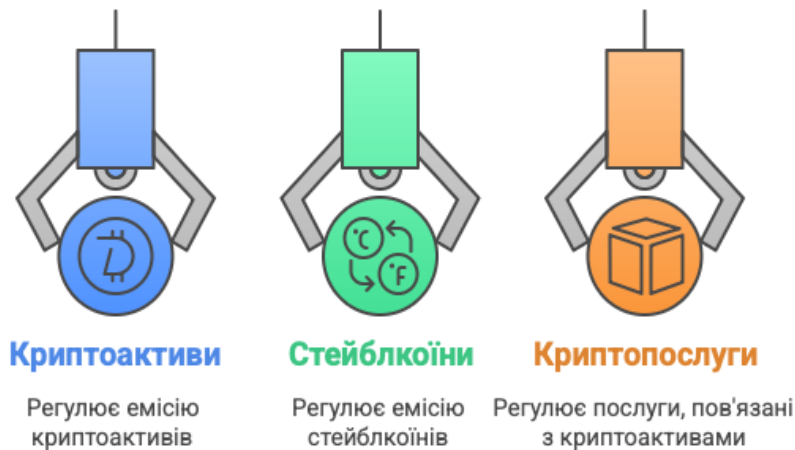
Тим часом ЄС запровадив окреме регулювання для токенів (званих у MiCAR «крипто активами») у вигляді «*Markets in Crypto Assets Regulation*»

⁷² Рішення суду SEC v. W.J. Howey Co., 328 U.S. 293 (1946). Для порівняння вимог США та ЄС див. Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Law, Chicago Journal of International Law 19 (2019), 547.

⁷³ BaFin. Guidance Notice, Second advisory letter on prospectus and authorisation requirements in connection with the issuance of crypto tokens. 2019. URL: <https://www.bafin.de/ref/19593866> (date of access: 30.04.2025).

(«MiCAR»)⁷⁴. MiCAR регулює токени як такі (хоча є винятки, такі як NFT, які не підпадають під дію MiCAR). Незважаючи на регулювання tokenів MiCAR, питання про віднесення їх до категорії фінансових інструментів у ЄС не вирішено. На думку ЄС, токени мають підлягати спеціальному регулюванню, але тільки в тому разі, якщо вони не кваліфікуються як фінансові інструменти за межами MiCAR. У своєму регулюванні ЄС дотримується принципу «технологічної нейтральності», який означає, що форма існування активу (наприклад, токен чи традиційний документ) не має вирішального значення для його регуляторної кваліфікації.

Що регулює MiCAR?



Відповідно, європейські наглядові органи також оприлюднили рекомендації щодо розмежування між токенами в значенні Регламенту MiCAR та фінансовими інструментами⁷⁵. Як емітенти tokenів, що підпадають під дію Регламенту MiCAR, так і емітенти tokenів, віднесених до категорії фінансових інструментів, зобов'язані дотримуватись різних нормативних вимог. До них, зокрема, відноситься публікація «Білої книги» (для tokenів) або «Проспекту емісії» (для фінансових інструментів), що мають містити інформацію про

⁷⁴ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

⁷⁵ ESMA. Final Report. Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. 2024. URL: https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf (date of access: 30.04.2025).

емітента і токен. Крім того, необхідно дотримуватися різних правил, спрямованих на запобігання зловживанням на ринку (наприклад, правила, що забороняють інсайдерську торгівлю тощо).

Незважаючи на те, що загалом правила регулювання фінансових інструментів і токенів схожі, між ними існує значна кількість відмінностей у деталях. Саме тому на практиці важливим є те, чи регулюється конкретний токен Регламентом MiCAR чи загальним законодавством про цінні папери.

Другий аспект фінансового регулювання стосується не самих токенів, а послуг, пов'язаних із ними. Оскільки паралельно з регульованим «традиційним» фінансовим ринком з'явився ринок токенів, на ньому активно надаються нові види послуг. Насамперед ідеться про депозитарні послуги (зберігання приватних ключів користувачів) та платформи для торгівлі токенами. Емісія окремих типів токенів, таких як стейблкоїни (*stablecoin*), що вже згадувалися в контексті платіжних токенів, за своїм характером наближається до регульованої фінансової діяльності. Стейблкоїни, зокрема, мають значну подібність до електронних грошей, емісія та обіг яких спеціально врегульовані в законодавстві ЄС.

Такі фінансові послуги та пов'язана з ними діяльність на фінансовому ринку зазвичай підлягають жорсткому регулюванню. У більшості правових систем постачальники фінансових послуг мають право розпочинати свою діяльність лише після отримання офіційного дозволу від компетентного наглядового органу. Для цього необхідно виконати низку нормативних вимог. Крім того, такі суб'єкти перебувають під постійним державним наглядом, який контролює дотримання встановлених правил.

Проте вказані правила застосовуються лише у випадках, коли відповідні положення поширюються на регульований продукт. Це питання не є тривіальним. До набуття чинності Регламентом MiCAR, у межах ЄС до таких регульованих продуктів переважно відносилися фінансові інструменти, а також електронні гроші та інші банківські послуги (наприклад, кредитування). Послуги, пов'язані з токенами, які не належали до фінансових інструментів, як правило, не підпадали під відповідне фінансове регулювання.

Разом з тим, токени створили новий ринок, який за своєю структурою нагадує традиційний фінансовий ринок і в багатьох аспектах перетинається з ним. Таким чином, необхідність у встановленні регуляторних рамок є очевидною.

Ця проблема наявна і в більшості інших правових систем. За таких обставин у США виникла судова справа, ініційована Комісією з цінних паперів та бірж (SEC), у якій стверджувалося, що токени слід кваліфікувати як фінансові інструменти, аби, зокрема, платформи для торгівлі токенами підпадали під регулювання фінансового ринку та контроль з боку SEC.

У Європейському Союзі це питання наразі врегульовано шляхом ухвалення Регламенту MiCAR. Паралельно з традиційним регулюванням фінансових ринків запроваджується і регулювання послуг, пов'язаних із токенами. Це регулювання багато в чому подібне до регулювання традиційної діяльності на фінансовому ринку, проте воно також адаптоване до специфіки токенів.

Аналогічні регуляторні тенденції спостерігаються в усьому світі. Уряд Великої Британії обговорює можливість запровадження відповідного регулювання, яке за своєю логікою нагадує MiCAR⁷⁶. Україна навіть пішла на крок уперед, ухваливши відповідний закон, проте його набрання чинності було поставлено у залежність від прийняття супровідного податкового законодавства, яке станом на сьогодні ще не затверджено⁷⁷. Таким чином, українське регулювання поки що не діє. Водночас за логікою регулювання воно також подібне до MiCAR, а запропоновані наразі зміни покликані ще більше наблизити українське законодавство до європейських стандартів⁷⁸.

⁷⁶ Див. план уряду Великої Британії: HM Treasury, Future financial services regulatory regime für cryptoassets, Consultation and call for evidence. February 2023. URL: https://assets.publishing.service.gov.uk/media/63d94ea68fa8f51881c99eb4/TR_Privacy_edits_Future_financial_service_s_regulatory_regime_for_cryptoassets_vP.pdf (date of access: 30.04.2025).

⁷⁷ Про віртуальні активи: Закон України № 2074-IX від 17 лютого 2022 року.

⁷⁸ Див. Olekhov/Ilchenko/Orlyk/Valyeyeva, CMS Expert Guide to Crypto Regulation in Ukraine, URL: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-crypto-regulation/ukraine> (дата звернення: 30.04.2025).

3.3. Супутні правові питання у контексті токенизації

У зв'язку з обігом.tokenів у різних юрисдикціях виникає широкий спектр додаткових правових питань, зокрема:

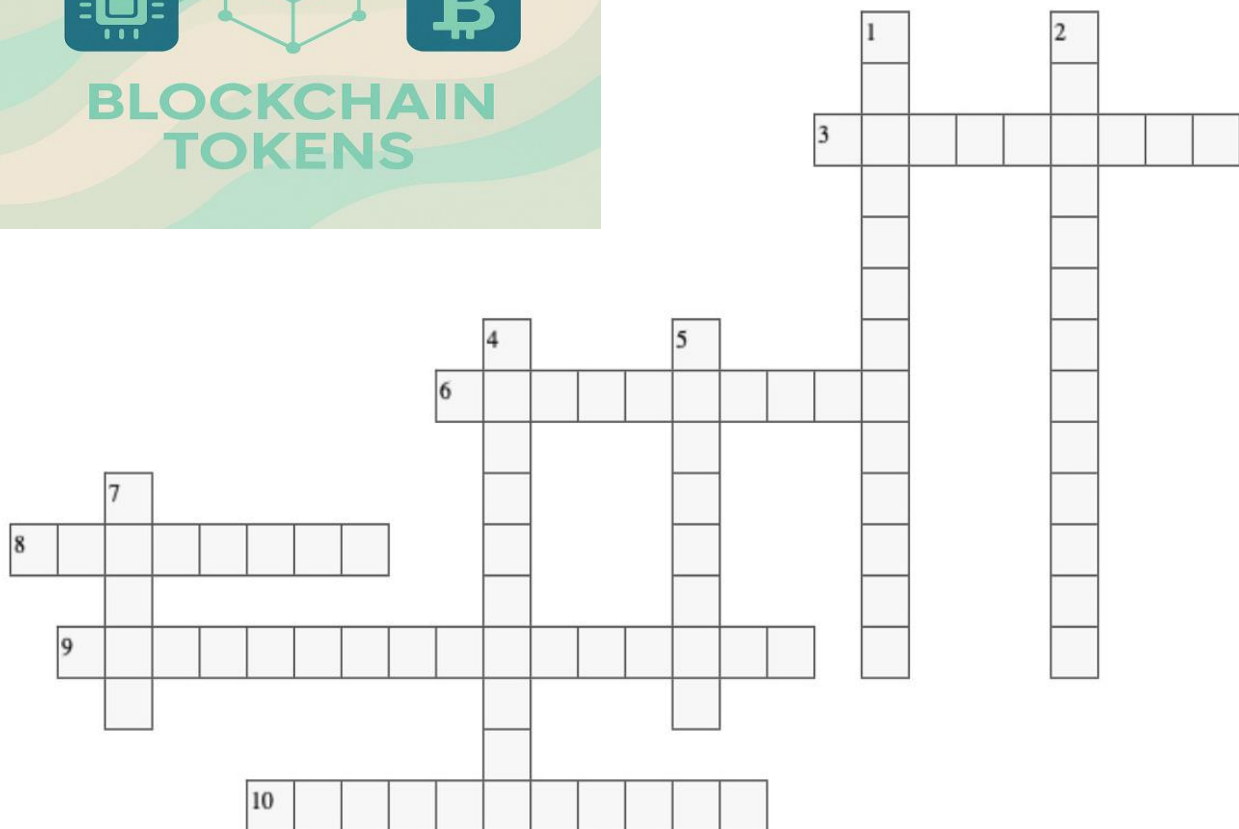
- Яке національне право застосовується до.tokenів?
- Як дотримуватися вимог щодо захисту персональних даних, якщо блокчейн має публічний, децентралізований характер?
- Яким чином можна запобігати відмиванню коштів?
- Який порядок оподаткування.tokenів?

Усі ці питання потребують не лише юридичної інтерпретації, але й, у багатьох випадках, спеціального законодавчого врегулювання.



ПЕРЕВІРКА ЗНАНЬ

Для закріплення пройденого матеріалу розв'яжіть кросворд.



По горизонталі

3. Юридичний термін для процесу перевірки трансакцій у блокчейні
6. Токени, ціна яких прив'язана до фіксованої еталонної вартості.
8. Модель мережі, де дані зберігаються без централізованого контролю.
9. Назва токenu, який є цифровим представленням права власності на унікальний об'єкт.
10. Процес перенесення реальних активів у цифрову форму на блокчейні.

По вертикалі

1. Програмний код на блокчейні, який виконується автоматично при виконанні умов.
2. Файл із кодом, у якому визначаються правила поведінки токена.
4. Тип токенів, які надають доступ до продуктів чи послуг.
5. Тип токенів, найчастіше пов'язаний із грошовими функціями.
7. Цифровий об'єкт, що не має матеріальної форми, але підтверджує право власності на актив у блокчейні.

ЗАВДАННЯ

1. Legal analysis: Can an NFT be considered an object of property rights under Ukrainian law?

Обґрунтуйте відповідь з урахуванням ЦК України. Підготуйте короткий виступ.



2. Comparative analysis of token regulation in the USA (Howey Test) and the EU (MiCAR).

Визначте сильні та слабкі сторони обох систем. Оформіть результати у вигляді презентації або інфографіки.



3. Legal Case: “Ape in a Hoodie – Who Holds the Rights?”

Олена купила NFT №4827 з колекції *Bored Ape Yacht Club*. Це мавпа з червоним капелюхом і сигарою. Вона вирішила створити бренд вуличного одягу «RedApe Wear» і надрукувала цю мавпу на футболках, худі та кепках, які почала продавати онлайн.

Через кілька місяців компанія «Urban Jungle Ltd» також випустила колекцію одягу з подібними зображеннями мавп з BAYC – але жоден із цих NFT їм не належав.

Questions:

1. Чи мала Олена право використовувати зображення NFT-мави в комерційних цілях?
2. Чи порушила компанія *Urban Jungle Ltd* авторські або майнові права?
3. Хто несе відповідальність: творець NFT, покупець чи сторонній користувач?



4. Legal Case: NFT and Property Rights

Ольга купила NFT-токен, який надає право власності на цифрову картину. Вона хоче використати це зображення для друку футболок і продажу їх на Etsy.

Questions:

1. Проаналізуй, чи має Ольга правову можливість комерційно використовувати зображення.
2. Які права вона отримує через NFT?
3. Чи потрібно їй додаткове ліцензування?

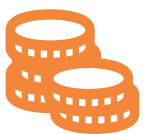


5. ICO and Legal Liability

Стартап з України провів ICO (Initial Coin Offering) для утилітарних токенів, зібравши 1 млн доларів. Продукт, який обіцяли створити, не реалізували через технічні проблеми.

Questions:

1. Чи може інвестор вимагати повернення коштів?
2. Яке правове поле застосовується до такої ситуації в Україні та ЄС?
3. Чи можна кваліфікувати токени як фінансові інструменти?



6. Stablecoins and Banking Regulation

Компанія хоче емітувати стейблкоїн, прив'язаний до гривні, для внутрішніх розрахунків у застосунку.

Questions:

1. *Чи прирівнюється такий стейблкоїн до електронних грошей?*
2. *Який регуляторний орган має дати дозвіл?*
3. *Які ризики та вимоги передбачає MiCAR або українське законодавство?*



7. Real Estate Tokenization

Інвестор пропонує токенизувати комерційне приміщення у Львові через смартконтракт, щоб кілька осіб володіли частками.

Questions:

1. *Чи визнає українське право такі частки об'єктом власності?*
2. *Як оформити правовий зв'язок між токеном і реальною нерухомістю?*
3. *Чи потрібна нотаріальна форма?*



8. Legal Grounds for the Claim

Клієнт купив токен, який обіцяв прибуток від участі в онлайн-платформі. Прибуток не був виплачений. Клієнт подає позов.

Questions:

1. *Як кваліфікувати токен: утилітарний чи інвестиційний?*
2. *Чи підпадає діяльність платформи під нагляд за фінансовими ринками?*
3. *Які докази має надати позивач для підтвердження своїх прав*

Розділ V СМАРТ-КОНТРАКТИ

SMART CONTRACTS

1. Поняття та сутність смарт-контрактів: від ідеї до практики

Смарт-контракт (англ. smart contract) – це комп’ютерний алгоритм, призначений для автоматичного виконання, контролю або документування юридично значущих подій відповідно до умов контракту. Вперше поняття було запропоноване Ніком Сабо у 1990-х роках, задовго до появи технології блокчейн⁷⁹.

Нік Сабо у 1994 році описав ідею цифрових контрактів, які самі виконуються без втручання третіх сторін. Приклад, який він сам навів як «прототип смарт-контракту», є автомат з продажу напоїв (вендинг-машина):  людина кидає монети, автомат перевіряє, чи достатньо грошей, видає вам товар, у разі помилки – повертає гроші.

Це звичайно є примітивним прикладом, але він показує суть смарт-контракту – дії виконуються автоматично, за заздалегідь запрограмованими умовами, і після того як запускається програма, змінити її хід неможливо⁸⁰.



Вперше реальне впровадження смарт-контрактів відбулося з запуском Ethereum у 2015 році.

Ethereum – це децентралізована блокчейн-платформа, створена для виконання смарт-контрактів і децентралізованих застосунків (dApps). Вона була

⁷⁹ Smart Contract Basics. URL: <https://stellar.org/learn/smart-contract-basics> (date of access: 10.04.2025).

⁸⁰ What are Smart Contracts Used For? URL: <https://www.futurelearn.com/info/courses/defi-exploring-decentralised-finance-with-blockchain-technologies/0/steps/251885> (date of access: 11.03.2025).

розроблена Віталіком Бутеріним, українсько-канадським програмістом⁸¹ та є однієї з найпопулярніших блокчейн-платформ у світі.

Перші смарт-контракти були дуже простими. Один із ранніх контрактів дозволяв людині надіслати Ether (ETH) і в обмін отримати токен. Ether (ETH) – це власна криптовалюта мережі Ethereum.

Токен – це цифровий актив, який випускається на основі блокчейн-платформи (в т.ч. Ethereum). Він є універсальним представником вартості, права або функції, який може виконувати найрізноманітніші ролі у цифровій екосистемі.

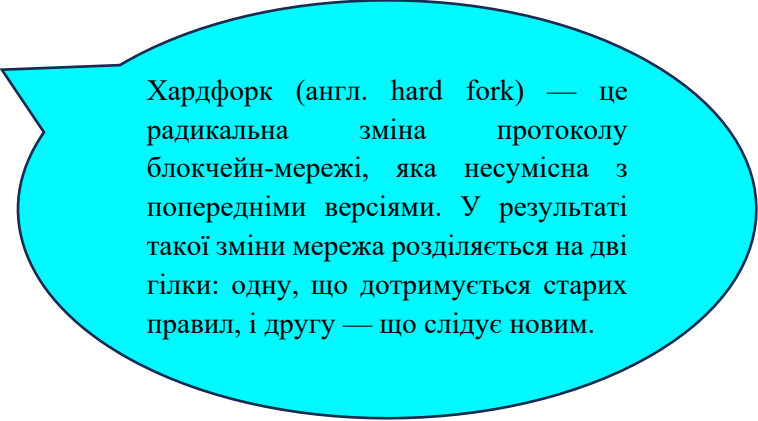
Також перші смарт-контракти використовувалися для обчислення простих лотерей, голосування або зберігали умовні депозити.

Не обійшлося на даному етапі і без інциденту, який став одним із найбільш знакових моментів в історії блокчейн-технологій, зокрема платформи Ethereum. В 2016 році як смарт-контракт на базі Ethereum був організований Decentralized Autonomous Organization (DAO). DAO була побудована як платформа для збору коштів через смарт-контракт, і її метою було створення децентралізованого венчурного капіталу. Учасники могли інвестувати Ether (ETH) у вигляді токенів DAO. В результаті її запуску вдалося залучити понад 150 мільйонів доларів, що на той час становило приблизно 14% від усієї циркулюючої кількості Ethereum. Але, як часто буває в світі нових технологій, код смарт-контракту DAO містив уразливість. Зловмисник скористався цією помилкою. Через механізм, який дозволяв робити «поновлення» токенів, він зміг двічі витягнути кошти з контракту, що призвело до викрадення близько 50 мільйонів доларів у вигляді ETH.

Спільнота Ethereum виявилася перед серйозним вибором — або прийняти ситуацію і дозволити DAO залишити кошти у руках зловмисника, або щось зробити для відновлення справедливості. Через значний вплив, було вирішено застосувати радикальний крок, який вплинув на репутацію і стабільність

⁸¹ What Is Ethereum and How Does It Work? URL: <https://www.investopedia.com/terms/e/ethereum.asp> (date of access: 11.04.2025).

Ethereum. Спільнота вирішила зробити хардфорк, який дозволив повернути викрадені кошти інвесторам. Це означало, що блокчейн Ethereum було «повернуто» до того моменту, коли кошти



Хардфорк (англ. hard fork) — це радикальна зміна протоколу блокчейн-мережі, яка несумісна з попередніми версіями. У результаті такої зміни мережа розділяється на дві гілки: одну, що дотримується старих правил, і другу — що слідує новим.

ще не були викрадені, і всі учасники DAO, хто втратив гроші, отримали назад свої інвестиції. Це рішення призвело до того, що частина учасників, зокрема ті, хто виступав за принципи децентралізації та незмінності блокчейну, виступили проти хардфорку. Вони вважали, що блокчейн не має права змінюватися через помилки, адже одна з основних рис криптовалют — це незмінність записів у блокчейні. Тому вони продовжили підтримувати Ethereum Classic (ETC) — оригінальну версію блокчейну без хардфорку.

В результаті, Ethereum розділилося на два окремі проекти:

- Ethereum (ETH) — з хардфорком, який повернув викрадені кошти;
- Ethereum Classic (ETC) — з оригінальним блокчейном без змін.

Цей інцидент став важливою віхою в розвитку криптовалют і блокчейн-технологій, оскільки він не тільки продемонстрував уразливості в смарт-контрактах, але й поставив важливі питання про управління і децентралізацію в світі блокчейнів⁸².

Ці приклади демонструють, як смарт-контракти пройшли шлях від теоретичних основ до ключового елементу сучасної криптоекономіки.

У сучасному розумінні смарт-контракт — це програмний код, який зберігається у децентралізованій блокчейн-мережі та виконується автоматично після настання відповідних передбачуваних умов.

⁸² Wikipedia. The DAO (Ethereum). URL: https://en.wikipedia.org/wiki/The_DAO (date of access: 01.04.2025).

2. Юридичний статус смарт-контрактів

Смарт-контракти мають великий потенціал для зміни способів ведення сучасного бізнесу та угод, але їх юридичний статус залежить від різних факторів, таких як юрисдикція, специфіка угоди, а також від того, чи відповідають вони чинному національному та міжнародному законодавству.

Смарт-контракти по суті є цифровими договорами, які автоматично виконують умови без необхідності залучення посередників або представників сторін. Ключовою особливістю є їх автоматизм і самовиконуваність на блокчейн-платформах.

Смарт-контракт може бути розглянутий як *форма цифрової угоди*, де правила і умови взаємодії між сторонами заcoded в програмному коді. Це робить процес виконання угоди більш прозорим і безпечним.

2.1. Співвідношення смарт-контракту та традиційного цивільно-правового договору на сучасному етапі



Смарт-контракт як технологічне явище не може автоматично розглядатися як цивільно-правовий договір у класичному розумінні, оскільки він не завжди відповідає базовим критеріям, що

характеризують традиційний договір. Зокрема, в окремих випадках смарт-контракт позбавлений чітко вираженого наміру сторін, їх згоди, визначеного предмета та інших ключових елементів, які традиційно формують зміст

договору. Додатковою складністю є відсутність належної ідентифікації учасників, що унеможливлює однозначне встановлення суб'єктного складу зобов'язання. Також програмний код, який є основою смарт-контракту, рідко відображає волевиявлення сторін у юридично зрозумілій і формалізованій формі, що ще більше ускладнює його трактування як повноцінного договору в юридичному сенсі.

Водночас смарт-контракт набуває значення як технічний засіб забезпечення належного виконання зобов'язань, які можуть виникати в межах або на підставі цивільно-правового договору. Його застосування сприяє автоматизації процесу виконання умов договору, мінімізує ризики їх порушення та може функціонувати як частина більш широкого механізму реалізації правовідносин, зокрема тих, що оформлені традиційними юридичними інструментами. Таким чином, смарт-контракт доцільніше розглядати не як самостійний договір, а як допоміжний інструмент, який виконує технічні функції у сфері правового регулювання.

2.2. Перспективи застосування смарт-контрактів у майбутньому в цивільних правовідносинах

Смарт-контракти мають великий потенціал для заміни традиційних юридичних договорів, але в тих випадках, коли потрібно автоматизувати виконання умов договору та мінімізувати роль посередників. Однак важливо зазначити, що смарт-контракти не завжди є ідеальним рішенням для кожного виду цивільно правового договору, оскільки вони мають свої обмеження, зокрема в складності угод та можливості виправлення помилок.

Розглянемо можливі приклади, коли традиційний договір може бути забезпечений смарт-контрактом.

Типові договори, які можуть бути автоматизовані смартконтрактом



Незважаючи на великий потенціал смарт-контрактів для автоматизації багатьох видів угод, існують деякі типи договорів, які не можуть бути замінені смарт-контрактами через їх складність, необхідність в інтерпретації чи судовому вирішенні спорів, а також через обмеження технології, і навіть бути використані як спосіб належного забезпечення виконання договору.



Отже, смарт-контракти мають великий потенціал для автоматизації багатьох аспектів традиційних угод, проте вони не можуть замінити всі типи договорів, особливо ті, що вимагають складної інтерпретації, судового вирішення спорів, захисту прав людини чи високого рівня конфіденційності. Тому смарт-контракти є лише інструментом для автоматизації певних видів угод, але не можуть повністю замінити всі традиційні юридичні процеси.

2.3. Юридичне визнання смарт-контрактів

У деяких країнах законодавство прямо визнає смарт-контракти як форму договору – тобто укладений у цифровій формі смарт-контракт має таку ж юридичну силу, як і традиційний письмовий договір. Однак є багато країн, де смарт-контракти не мають чіткої правової визначеності, що створює проблеми в разі конфліктів та здійсненні судового захисту порушених прав та інтересів, оскільки суд може не визнати його як доказ або не надати йому сили зобов'язання.

Країни, що визнають смарт-контракти



2.4. Юрисдикція та міжнародний аспект застосування смарт-контрактів

Смарт-контракти можуть порушувати питання юрисдикції, оскільки одна і та сама угода може підпадати під законодавство різних країн в залежності від місця проживання учасників угоди або платформи, на якій вона реалізується. Це може ускладнити правове вирішення спорів, оскільки різні країни мають різну законодавчу базу щодо врегулювання використання криптовалюти і технологій блокчейн.

В країнах Європи та США, діють жорсткі вимоги щодо захисту прав споживачів, конфіденційності даних (наприклад, GDPR в ЄС). Смарт-контракти повинні враховувати ці вимоги, щоб не порушувати законодавство про захист даних або фінансове законодавство.

2.5. Проблеми щодо захисту порушених прав та інтересів користувачів смарт-контрактів

Оскільки смарт-контракти автоматизують виконання угод без участі людини, можуть виникнути ситуації, коли одна зі сторін не згодна з результатом виконання контракту. Однак, через те, що виконання угоди здійснюється на децентралізованих платформах, це може ускладнити вирішення спорів через традиційні судові системи.



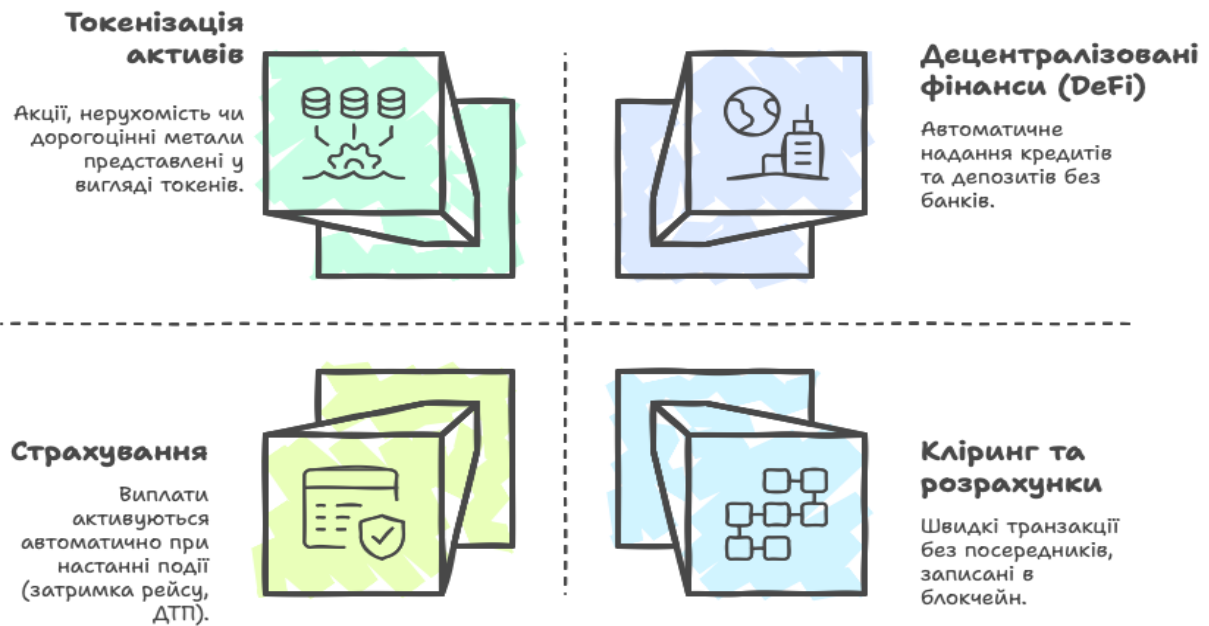
Що робити, якщо в смарт-контракті є помилка або несправедливе виконання умов? Враховуючи, що смарт-контракти є незмінними після їх запуску, можуть виникати ситуації, коли помилки не можна виправити без втручання в код блокчейну, що може призвести до спорів, які не мають механізмів вирішення.

Отже, юридичний статус смарт-контрактів є складним і залежить від багатьох факторів, зокрема від конкретної юрисдикції та виду угоди. Однак їх автоматизований характер і здатність виконувати умови без посередників робить їх привабливими для застосування в різних сферах. Проте для того, щоб вони стали частиною традиційної правової системи, необхідно подолати ряд правових і технічних бар'єрів.

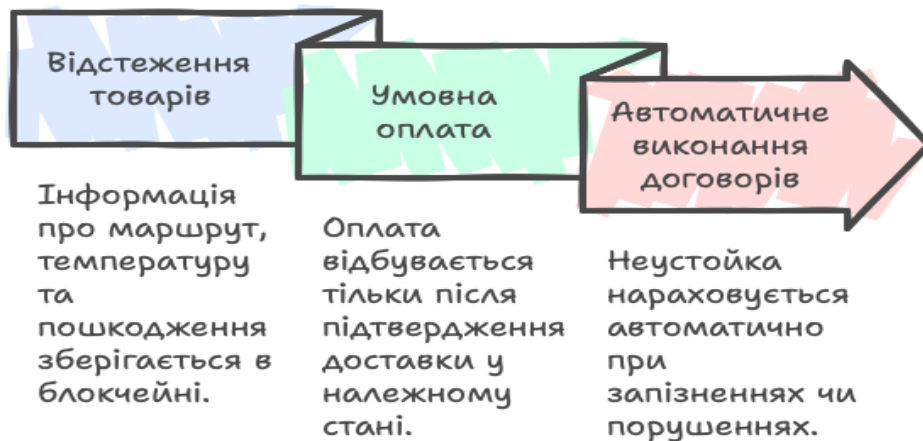
3. Сфери застосування смарт-контрактів

Смарт-контракти вже зараз активно використовуються у різних сферах, і найбільш ефективними вони виявляються там, де потрібна прозорість, автоматизація та зниження людського втручання.

Фінансовий сектор



Логістика та постачання



Смарт-контракти – це не майбутнє, а вже реальність, і що далі, то більше галузей їх інтегрує. Смарт-контракти не замінять всю сферу застосування типових договорів до яких ми звикли, але доповнять їх там, де можна автоматизувати довіру.



ПЕРЕВІРКА ЗНАНЬ

What is true and what is false?

Justify your answer.

1. Смарт-контракт був уперше реалізований на блокчейн-платформі Bitcoin.
2. Ідея смарт-контрактів була

запропонована Ніком Сабо ще до появи блокчейн-технологій.

3. Ethereum був створений спеціально для виконання смарт-контрактів та децентралізованих застосунків.

4. Уразливість смарт-контракту DAO у 2016 році призвела до викрадення понад 150 мільйонів доларів у вигляді ETH.

5. Після інциденту з DAO, блокчейн Ethereum залишився незмінним.

6. Ethereum Classic утворився як результат незгоди частини спільноти з рішенням зробити хардфорк.

7. Смарт-контракт автоматично виконується після настання заданих умов і не може бути змінений після запуску.

8. Смарт-контракт завжди вважається цивільно-правовим договором за будь-якої юрисдикції.

9. У деяких країнах смарт-контракти визнаються юридично рівноцінними до письмових договорів.

10. Однією з проблем смарт-контрактів є складність виправлення помилок після їх активації.

ЗАВДАННЯ

**1. Legal Analysis: A Task for Legal Professionals**

Здійсніть дослідження щодо правового аналізу юридичного статусу смарт-контрактів, надавши відповіді на наступні питання:

- *Юридична сила смарт-контракту на території нашої держави.*
- *Правове регулювання застосування смарт-контракту національним законодавством.*
- *Основні принципи роботи смарт-контрактів.*
- *Провести порівняльний аналіз понять смарт-контракт та цивільно-правовий договір.*
- *Зробити висновки щодо можливих проблем застосування смарт-контрактів у договірних відносинах та запропонувати шляхи їх вирішення.*
- *Провести порівняльний аналіз юридичного статусу смарт-контрактів в Україні з іншими країнами (наприклад, США, ЄС).*

**2. Debate: «Smart-contract will replace civil law contract?»**

Підготуйте аргументи для проведення дебатів щодо того, чи зможе смарт-контракт замінити традиційний цивільно-правовий договір.

**3. Smart contract in the field of cryptocurrencies**

Розробіть модель застосування смарт-контракту у зобов'язальних відносинах, які виникають із простого фінансового договору між двома сторонами, що здійснюють операції за допомогою криптовалюти. Алгоритм виконання завдання:

1. *Створити умови договору (наприклад, умови про покупку-продаж за криптовалютою).*
2. *Описати, які юридичні аспекти варто врахувати при складанні смарт-контракту для криптовалютних транзакцій. Як юридично оформити умови, що містяться в смарт-контракті.*

3. *Визначити правові наслідки, якщо одна зі сторін не виконує умови договору.*

4. *Проаналізувати можливості для вирішення спорів, зокрема у випадку несанкціонованих змін в коді смарт-контракту.*



4. Smart Contract in the Field of Intellectual Property

Як на вашу думку можна застосувати смарт-контракт у сфері управління майновими правами на інтелектуальну власність.

1. *Опишіть, як смарт-контракт може бути використаний.*
2. *Опишіть механізм захисту прав інтелектуальної власності.*
3. *Проаналізуйте, які юридичні аспекти можуть виникнути при використанні смарт-контрактів в цій сфері.*



5. Use of Smart Contracts in Public Administration

Поміркуйте як смарт-контракти можуть бути використані в публічному секторі, наприклад, для автоматизації адміністративних процесів (виплата субсидій, податкові декларації, публічні закупівлі).

1. *Опишіть можливі сценарії застосування смарт-контрактів у публічному секторі.*
2. *Проаналізуйте юридичні та етичні аспекти застосування смарт-контрактів для державних послуг.*
3. *Розгляньте, чи може смарт-контракт замінити або доповнити традиційні юридичні процедури.*
4. *Як можна забезпечити відповідність смарт-контрактів законодавству та етичним стандартам у публічному секторі?*
5. *Які переваги та ризики можуть виникнути при застосуванні смарт-контрактів в державних закупівлях?*

Розділ VI ШТУЧНИЙ ІНТЕЛЕКТ

ARTIFICIAL INTELLIGENCE

1. Поняття та основні форми штучного інтелекту

Сьогодні, свідомо чи ні, більшість людей уже мають досвід взаємодії зі штучним інтелектом (далі ШІ). Так, технології ШІ інтегровані у повсякденні сервіси, такі як: пошукові системи (Google), соцмережі (Facebook, Instagram), стримінгові платформи (Netflix, YouTube), онлайн-магазини (Amazon), цифрові помічники (Siri, Alexa), чат-боти банків чи служб підтримки. Багато хто з користувачів навіть не усвідомлює, що за відповідними сервісами стоїть ШІ.

Розвиток технологій штучного інтелекту настільки динамічний, що вже давно вийшов за межі суто технічних галузей, охопивши й традиційно консервативну юридичну сферу, де трансформує підходи до аналізу, прийняття рішень і надання правових послуг.



Ці приклади — не футуристичні гіпотези, а реальність, яка вже змінює юридичну практику в усьому світі. У центрі цієї трансформації — **штучний інтелект**. Саме тому студенти-юристи вже повинні бути знайомі з цими технологіями. Адже:



1. ШІ впливає на всі галузі права.

Алгоритмічне прийняття рішень ставить нові виклики у кримінальному, адміністративному, трудовому, фінансовому, договірному праві. Юристи мають розуміти, як ці технології працюють і які в них можуть бути ризики.

2. Потрібен новий рівень юридичного аналізу.

Як гарантувати, що ШІ не дискримінує? Як забезпечити прозорість рішень, ухвалених машиною? Яка відповідальність за шкоду, заподіяну системою на базі ШІ? Це нові правові питання, які потребують нових підходів.

3. Юристи мають брати участь у розробці правил для ШІ.

Закони і нормативні акти не встигають за розвитком технологій. Правники повинні бути серед тих, хто створює правові рамки для розвитку ШІ — етичні, безпечні та справедливі.

4. ШІ змінює юридичну професію.

Автоматизація рутинних завдань (пошук судової практики, підготовка документів, аналіз договорів) змінює роль юриста. Той, хто не володіє цифровими навичками, ризикує залишитися поза професією.

5. Глибше розуміння прав людини у цифрову епоху.

Право на приватність, захист персональних даних, право на пояснення автоматизованого рішення — усе це вимагає нової юридичної чутливості та фахових знань.

Definition

Відповідно до п.1 ст.3 Глави 1 AI Act (ЄС), термін «система ШІ» означає машинну систему, розроблену для функціонування з різними рівнями автономності, яка після впровадження може виявляти здатність до адаптації і яка, з урахуванням явних або неявних цілей, робить висновки на основі отриманих вхідних даних щодо того, як генерувати вихідні результати — такі як прогнози, контент, рекомендації або рішення, — що можуть впливати на фізичне або віртуальне середовище.

Простішими словами можна сказати, що Штучний інтелект — це здатність комп'ютерних систем виконувати завдання, які зазвичай вимагають людського інтелекту: аналізувати дані, розпізнавати мову, приймати рішення, навчатися на прикладах. Найпоширеніші сьогодні форми ШІ — це *машинне навчання*, *обробка природної мови* (наприклад, ChatGPT) і *комп'ютерний зір* (наприклад, розпізнавання облич).



Для того, щоб мати змогу юридично оцінювати перспективи та ризики штучного інтелекту, потрібно спочатку хоча б поверхово зрозуміти технічну складову технології штучного інтелекту. Тому детальніше зупинимось на найпоширеніших формах ШІ:

1. **Машинне навчання (Machine Learning, ML)** — фундамент.

Машинне навчання — це підхід, за якого *алгоритм самостійно навчається* на даних. Тобто, замість того щоб задавати комп'ютеру чіткі інструкції, йому надають дані, і він сам виводить закономірності, правила, структури. Це технологічний «двигун», який використовується в дуже багатьох сферах, включаючи NLP, комп'ютерний зір, рекомендаційні системи, медицину, фінанси тощо.

2. **Обробка природної мови (Natural Language Processing, NLP)** — ґрунтується на ML.

NLP — це *застосування машинного навчання до тексту та мови*, спеціалізується виключно на роботі з мовою: аналіз текстів, витяг ключових понять, машинний переклад, побудова чат-ботів, автоматичне резюмування та генерація відповідей.

NLP використовує алгоритми машинного навчання, особливо глибокі нейронні мережі (Deep Learning), щоб зрозуміти семантику, синтаксис, контекст тощо.

3. **Комп'ютерний зір (Computer Vision, CV)** – це напрям штучного інтелекту (на основі машинного навчання), який дозволяє машинам *«бачити» та інтерпретувати візуальну інформацію* так, як це робить людина. За допомогою комп'ютерного зору стає можливим:

- Розпізнавання облич і емоцій (розпізнавання емоцій часто використовувалось роботодавцями щодо своїх працівників, розпізнавання облич найчастіше використовується правоохоронними органами, наразі в ЄС заборонено, окрім встановлених винятків);
- Читання тексту з зображення (наприклад, із паспортів або фото рішень);
- Розпізнавання номерних знаків (платформи автоматизованої фіксації порушень ПДР (камери на дорогах) використовують комп'ютерний зір для розпізнавання номерів авто та ідентифікації порушень);
- Виявлення об'єктів — зброї, людей, документів тощо (найчастіше правоохоронними органами);

- Візуальний контроль якості (у промисловості та судовій експертизі).

4. Генеративний ШІ (Generative AI) — просунутий результат еволюції ML + NLP.

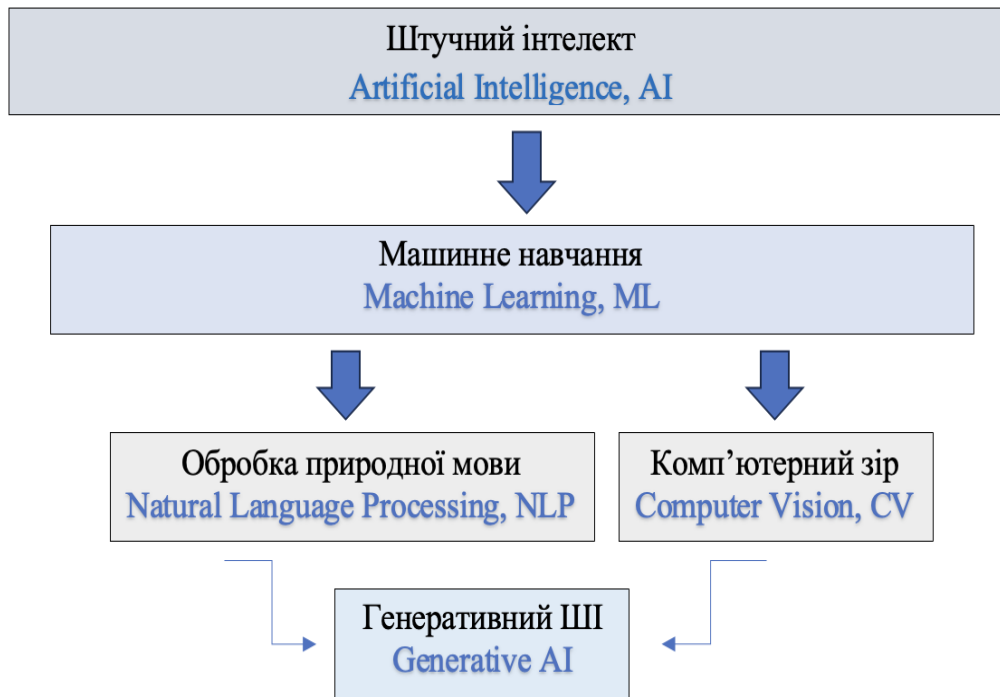
Генеративний ШІ — це система, яка *створює новий контент*: текст, зображення, відео, музику, код. Примітно, що генеративний ШІ — це сімейство інструментів, де LLM — найпоширеніший у праві, але не єдиний. Технології швидко розвиваються, і вже є прецеденти, коли юристи за кордоном працюють не лише з текстами, а й із згенерованими відео, доказами, реконструкціями подій⁸³. Різноманітність видів генеративного ШІ наочно представлено в таблиці.

Types of generative AI

Тип генеративного ШІ	Що генерує	Приклади	Галузі застосування
LLM (Large Language Models)	 Текст	GPT-4, Claude, Gemini	Юриспруденція, освіта, журналістика
Text-to-Image	 Зображення зі слів	DALL·E, Midjourney, Stable Diffusion	Дизайн, реклама, освіта
Text-to-Video	 Відео зі сценарію	Sora (OpenAI), Runway, Pika	Кіно, медіа, презентації
Text-to-Audio / Speech	 Звук, мову	ElevenLabs, Whisper, Play.ht	Озвучка, дубляж, подкасти
Text-to-Music	 Музику, мелодії	AIVA, Soundraw, Riffusion	Композиторство, фонові музика
Code generation	 Код	GitHub Copilot, CodeWhisperer	Програмування, ІТ-право
3D-моделі	 3D-об'єкти	Point-E, Meshy	Архітектура, ігри, цифрова експертиза
Data generation	 Нові дані або симуляції	Gretel.ai, Mostly AI	Тестування систем, симуляції справ
Мультимодальні моделі	 Комбінація кількох типів	GPT-4V (текст + зображення), Gemini	Юридична аналітика документів із графіками, фото тощо

З метою кращого розуміння співвідношення вище наведених понять їх наочно зображено у схемі:

⁸³ Fouraté, S. (n.d.). Lebenslange Haft für 25-Jährigen nach tödlichem Raserunfall in Wiesbaden. *Hessenschau*. URL: <https://www.hessenschau.de/panorama/lebenslange-haft-fuer-25-jachrigen-nach-toedlichem-raserunfall-in-wiesbaden-v3,raser-prozess-wiesbaden-100.html> (date of access 23.03.2025).



2. Інструменти ШІ в правовій сфері

1. Пошук правової інформації та аналітика.

Системи юридичного дослідження (наприклад, *Liga360 (Ukraine)*, *LexisNexis (USA, UK, Canada, and Australia)*, *CaseText (USA)*) використовують обробку природної мови для швидкого пошуку судової практики, норм законодавства, правових висновків.

Приклад: Адвокат вводить фразу «відповідальність за розірвання договору оренди», і система пропонує релевантні справи, тексти рішень судів та аналізує аргументи сторін.

2. Аналіз та складання юридичних документів.

Юридичні асистенти на базі ШІ можуть автоматично створювати шаблони договорів, заяв, позовів, надаючи рекомендації з формулювання і юридичного змісту.

Приклад: Платформа *DoNotPay* у США допомагає користувачам складати скарги на штрафи, заяви до страхової чи роботодавця, не залучаючи юриста. В

Україні також функціонує подібне: чатбот-консультант Правомен  (створює юридичні документи за символічну оплату, а також консультує);

БамперБот  розроблений колишнім поліцейським для водіїв, які потрапили в ДТП та консультує про порядок подальших дій; Устим бот  орієнтує у виборчому процесі.

3. Прогнозування судових рішень.

Деякі системи аналізують тисячі судових рішень і надають ймовірність перемоги у справі залежно від суду, складу суддів, типу позову та інших параметрів.

Приклад: В Україні є доступною система прогнозування судових рішень Verdictum PRO на базі ЛІГА: ЗАКОН.

4. Підтримка суддів і судових рішень.

У деяких юрисдикціях, наприклад у США, судді використовують алгоритми ризику рецидиву (*COMPAS*) для визначення доцільності звільнення під заставу або призначення запобіжного заходу.

Приклад: Система аналізує вік, попередні правопорушення, соціальні фактори — і пропонує «рівень ризику» повторного злочину. Це один із найспірніших напрямів, бо постає питання дискримінації, непрозорості та упередженості таких алгоритмів⁸⁴.

5. Розв'язання спорів онлайн (ODR).

Онлайн-платформи з використанням ШІ (наприклад, *eBay*, *Alibaba*) пропонують автоматичне врегулювання спорів між продавцем і покупцем, використовуючи попередні кейси та шаблони поведінки.

Приклад: Якщо покупець скаржиться на неотримання товару, система автоматично перевіряє факти, пропонує рішення (повернення коштів, нову відправку) й іноді ухвалює рішення без втручання людини.

⁸⁴ Dressel J., Farid H., The accuracy, fairness, and limits of predicting recidivism. *Science Advances*. 4, eaao5580 (2018). URL: <https://www.science.org/doi/10.1126/sciadv.aao5580> (date of access 23.03.2025).

6. Виявлення підозрілих трансакцій та комплаєнс.

У банківській та фінансовій сферах ШІ виявляє аномальні або потенційно незаконні операції, що може мати значення для правників у сфері AML (anti-money laundering).

Приклад: Юридичний департамент великої компанії отримує попередження про підозрілу угоду — і розпочинає внутрішнє розслідування ще до втручання правоохоронних органів.

Отже, з вище наведеного можна зробити висновок, що ШІ не замінює юриста повністю, але він стає потужним інструментом у його роботі. Роль правника в цьому контексті трансформується: він дедалі більше контролює, аналізує, оцінює рішення машин, і делегує ШІ рутинні завдання. Тому юридична освіта має бути адаптована до нової реальності.

3. Основні ризики використання ШІ в юриспруденції та виклики для правового регулювання

Розвиток штучного інтелекту створює не лише нові можливості, а й **реальні ризики** для прав людини, принципів правової держави, верховенства права і справедливості. Юрист повинен не лише використовувати нові інструменти, а й розуміти їх потенційні загрози.

Нижче подано ключові юридично значущі ризики у сфері застосування ШІ:

1. Непрозорість та «чорна скринька» (black box). Складні алгоритми, особливо в системах глибокого навчання, працюють як «чорна скринька»: вони приймають рішення без чіткого пояснення причин.

Правовий ризик: Порухення **права на пояснення** (особливо згідно зі статтею 22 GDPR) і, пов'язане з ним, **право на захист** — особа не може оскаржити або зрозуміти автоматизоване рішення, якщо не знає, як воно ухвалювалося.

2. Алгоритмічна дискримінація та упередженість (bias). Алгоритми вчаться на даних — а дані можуть бути упередженими (наприклад, історично расово чи соціально несправедливими). Наприклад, система COMPAS у США була розкритикована за те, що вона передбачала вищий ризик рецидиву для темношкірих обвинувачених; компанія Amazon припинила використання розробленого нею ШІ для рекрутингу, оскільки виявилось, що він відхиляв жіночі резюме через гендерну упередженість, бо навчався на резюме, де домінували чоловіки⁸⁵.

Правовий ризик: **Порушення принципу рівності перед законом, заборони дискримінації та справедливого суду.**

3. Використання без належного контролю людини. Унаслідок активного використання інструментів штучного інтелекту в людини знижується усвідомлення необхідності перевірки їх результатів. Італійський юрист і професор Нікола Фабіано (Nicola Fabiano) у своїй статті описує чотири судові випадки, коли адвокати подали суду вигадані факти, згенеровані ChatGPT, не перевірявши їх достовірність⁸⁶.

Правовий ризик: подання недостовірної інформації до суду, може кваліфікуватися як **порушення етичних стандартів професійної діяльності адвоката, спричинити дисциплінарну відповідальність**, а в окремих випадках — вплинути на **законність судового рішення**. Крім того, використання ШІ без належного контролю створює ризик **порушення принципу достовірності доказів**, а також ставить під сумнів легітимність правозастосування в цілому.

4. Порушення приватності та зловживання персональними даними. У процесі використання, ШІ може обробляти велику кількість даних, зокрема, персональних та чутливих (наприклад, відомості про здоров'я, доходи,

⁸⁵ Dastin J. Insight - Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. URL: <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/> (date of access 23.03.2025).

⁸⁶ Nicola Fabiano. AI Act and Large Language Models (LLMs): When critical issues and privacy impact require human and ethical oversight. *arXiv*, 2024. URL: <https://arxiv.org/html/2404.00600v1> (date of access 23.03.2025).

судимості). Зазвичай така інформація збирається та зберігається певний час організацією-розробником або провайдером сервісу.

Правовий ризик: **Порушення права на приватність, право «бути забутим» і захист персональних даних** (зокрема, у контексті GDPR).

5. Кіберзагрози та зловживання системами ШІ. Хакерські атаки на алгоритми, маніпуляція вихідними даними, використання ШІ у фішингових або маніпулятивних цілях — усе це відкриває нові вектори **кіберризиків**.

Правовий ризик: **Необхідність зміцнення цифрової безпеки, юрисдикційна невизначеність** у випадку транснаціональних кіберзлочинів, можливість обходу систем виявлення фішингу чи шахрайства, **загроза порушення права на приватність** через незаконне використання персональних даних.

Хоча цей перелік можна продовжувати, уже наведеного достатньо для усвідомлення якісно нових тенденцій, що постають у сфері юридичної науки та практики. Використання штучного інтелекту в праві не може бути безумовно позитивним або негативним — усе залежить від контексту, якості реалізації, прозорості алгоритмів та правового контролю. Юристи повинні стати «сторожами» алгоритмів, щоб ШІ працював на користь людини, а не всупереч її правам.

4. Правове регулювання ШІ в ЄС та Україні



1 серпня 2024 року в ЄС набув чинності перший у світі комплексний нормативно-правовий акт про штучний інтелект – Artificial Intelligence Act (AI Act). Він встановлює єдине на території ЄС правове регулювання ШІ, яке ґрунтується на людиноцентризмі та ризико-орієнтованому підході. Людиноцентризм означає, що технології мають

служувати людині, не порушувати її гідність, свободу, безпеку та основні права. Ризико-орієнтований підхід до регулювання ШІ – є спробою забезпечити достатню свободу для розвитку відповідних інновацій при одночасному забезпеченні основних прав і свобод людини-користувача. Тому, відповідно до AI Act, системи штучного інтелекту поділяються на чотири категорії залежно від рівня ризику, який вони становлять.

Категорія	Приклади	Статус
Заборонені системи	Системи соціального скорингу, маніпуляція поведінкою, біометричне стеження в реальному часі в публічних місцях (з певними винятками)	Заборонені
Високий ризик	ШІ в критичних сферах: правосуддя, охорона здоров'я, освіта, міграція, інфраструктура	Дозволено лише з суворим контролем
Обмежений ризик	Системи з впливом на права (наприклад, чат-боти)	Потрібна прозорість і попередження користувача
Мінімальний ризик	Ігри, фільтри в соцмережах	Без спеціального регулювання

Немає потреби детально зупинятись на заборонених системах ШІ, однак базове ознайомлення з ними є необхідним, тому надається зведена інформація в інфографіці нижче відповідно до ст.5 Глави II AI Act.

Заборонені системи штучного інтелекту



Системи ШІ високого ризику варто розглянути детальніше. Нижче в інфографіці представлено їх перелік відповідно до Додатку III AI Act.

Системи ШІ високого ризику



Біометричні системи

Методи віддаленої ідентифікації та категоризації, розпізнавання емоцій.

Системи ШІ, які використовуються як елементи безпеки у цифровій інфраструктурі, управлінні дорожнім рухом, постачанні води, газу, тепла, електроенергії.

Критична інфраструктура



Визначення доступу до навчальних закладів, оцінювання результатів навчання, визначення рівня освіти, який може отримати особа, виявлення порушень під час іспитів.



Доступ до освіти

ШІ, які здійснюють рекрутинг, аналіз анкет, прийняття рішень щодо умов, звільнення, просування, розподілу завдань, моніторингу продуктивності працівників.

Управління працевлаштуванням



Оцінка права на соціальну допомогу, медичні послуги, кредитоспроможності (крім виявлення шахрайства), страхова оцінка ризику (життя, здоров'я), пріоритезація екстрених викликів.



Доступ до послуг

Використання ШІ в оцінці ризику вчинення злочину, стати жертвою злочину, оцінці надійності доказів, профілювання осіб у кримінальному процесі, поліграфи або подібні засоби.

Правоохоронна діяльність



Оцінка безпекових чи міграційних ризиків, розгляд заяв на візи, притулок, дозволи на проживання; виявлення, розпізнавання чи ідентифікація осіб (крім перевірки проїзних документів).



Міграція, притулок, контроль кордонів

Підтримка судових органів у дослідженні фактів, тлумаченні та застосуванні норма права; вплив на результати виборів або голосування (крім адміністративного супроводу кампаній).

Судочинство та демократичні процеси



Ключовими **вимогами** до систем штучного інтелекту **високого ризику** є:

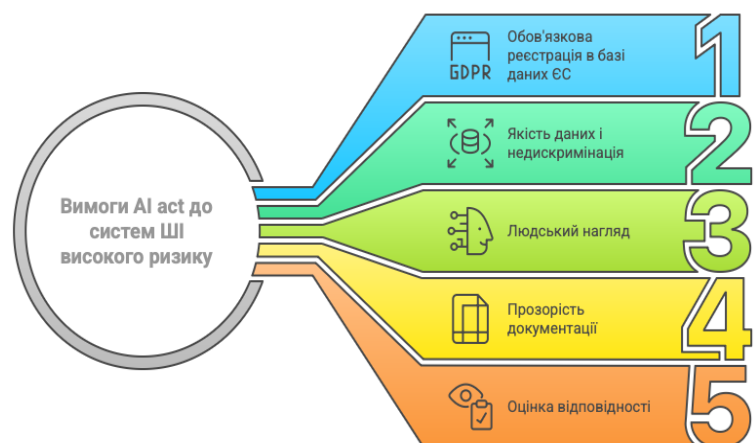
1. **Обов'язкова реєстрація таких систем в базі даних ЄС**, яку адмініструє Європейська комісія. Це забезпечує можливість моніторингу з боку ЄС та громадськості, сприяння відстеженню та аналізу використання таких технологій на території ЄС, а також публічну прозорість;

2. Вимоги до **якості даних та недискримінації**, тому такі системи мають базуватись на легальних, якісних, репрезентативних, точних і актуальних даних, які гарантуватимуть уникнення системної дискримінації, рівне ставлення до всіх користувачів, а також зменшення похибок у результатах;

3. **Запечечення людського нагляду** означає, що такі системи не можуть функціонувати повністю автономно без ефективного контролю з боку людини. Це включає: можливість втручання у процес прийняття рішень; наявність засобів контролю або скасування рішення прийнятого системою; обов'язкову участь людини в критичних етапах взаємодії з ШІ;

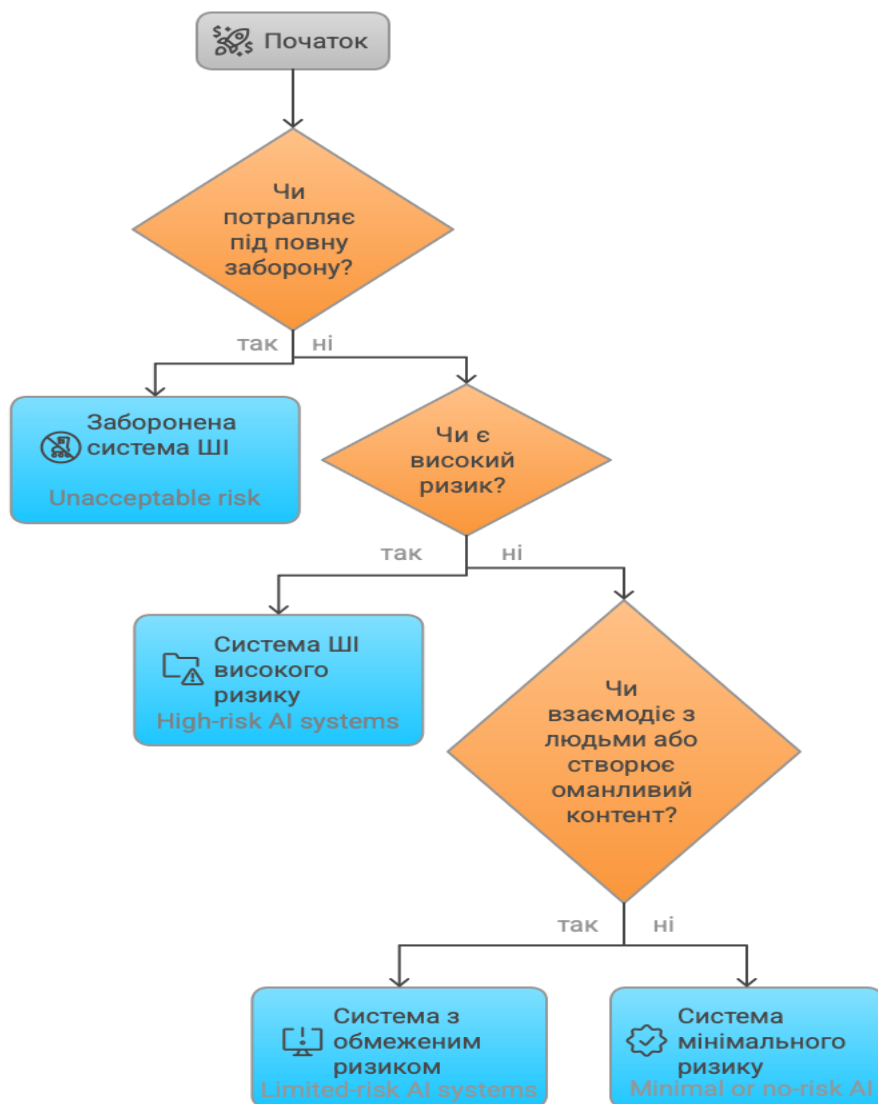
4. **Технічна документація і прозорість**. Розробники повинні створити повну технічну документацію, що містить: опис архітектури системи, алгоритмів, цілей використання; джерела та характеристики використаних даних; оцінку ризиків; способи забезпечення відповідності вимогам законодавства. Прозорість означає, що користувач при взаємодії з ШІ має бути повідомлений, що рішення приймає саме ШІ.

5. Проведення **оцінки відповідності**. Перш ніж система потрапить на ринок, розробник зобов'язаний провести процедуру відповідності, яка підтверджує, що система: відповідає вимогам законодавства ЄС; є безпечною; враховує права та інтереси людини.



Примітно, що відповідно до AI Act немає чіткого визначення систем ШІ, які належать до групи обмеженого ризику. Таке визначення залежить від аналізу функціональної здатності відповідної системи. Якщо система ШІ не загрожує напямую правам людини, а здійснює лише вплив на неї або її можливості, то така система відноситиметься до *Limited-risk AI systems* (наприклад, чат-боти, deepfakes).

Як визначити рівень ризику системи ШІ відповідно до AI Act?



Ключовою особливістю *Limited-risk AI systems* є **законодавча вимога забезпечення прозорості** їхнього використання. Це означає, що користувач має бути чітко поінформований, що він взаємодіє із системою штучного інтелекту. Зокрема, якщо йдеться про віртуального асистента або чат-бота, користувач повинен знати, що спілкується не з людиною. У випадку, коли зображення

(наприклад, deepfake), текст (зокрема новинного характеру) або інший контент створено за допомогою ШІ, він має бути належним чином промаркований, щоб користувач розумів, що цей контент є результатом генерації ШІ.

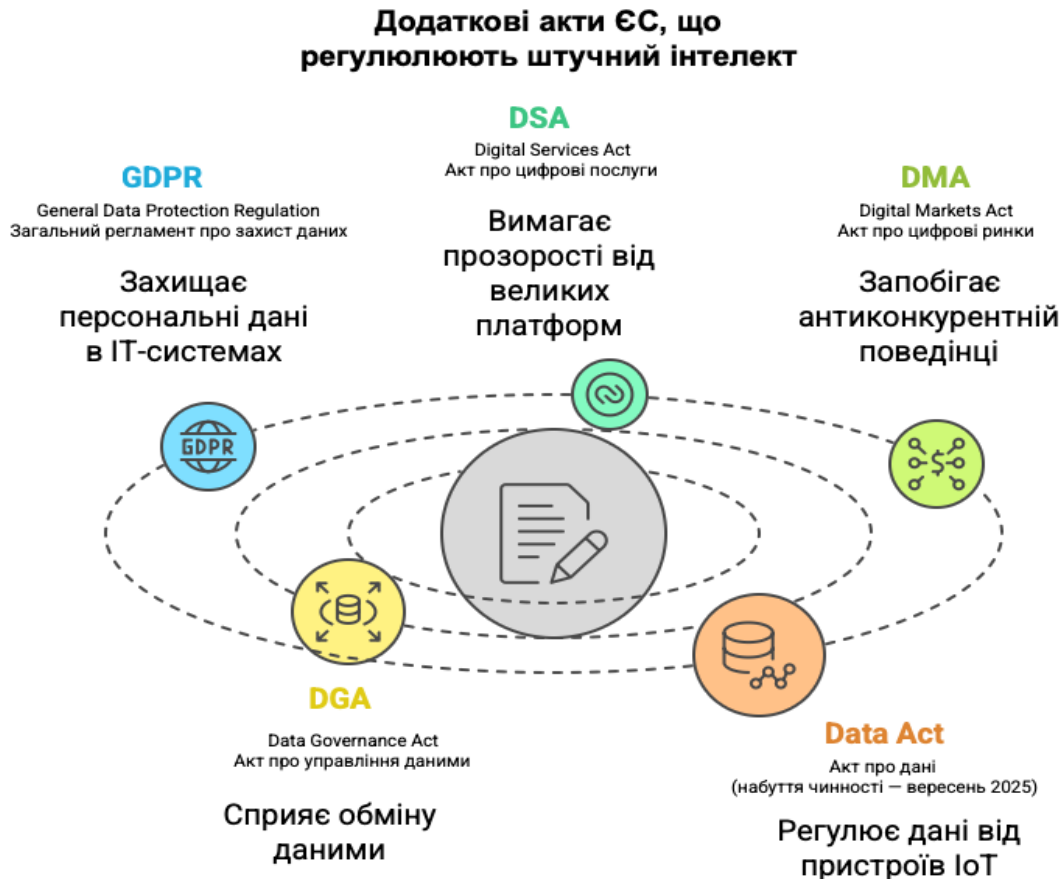
Що стосується *Minimal or no-risk AI*, то вони не підпадають під обов'язкові вимоги AI Act, оскільки не мають значного впливу на безпеку, права чи свободи людини. Їхнє використання дозволене без спеціальних обмежень або реєстрації. До них відносяться, зокрема, системи фільтрації спаму, комп'ютерні ігри, системи рекомендацій товарів та ін.

Не дивлячись на проривний характер AI Act, він, водночас, зазнав чимало критики. На міжнародному рівні Сполучені Штати Америки та Сполучене Королівство також не підписали декларацію щодо безпечного та інклюзивного використання штучного інтелекту. Це підкреслило розбіжності в підходах до регулювання ШІ між цими країнами та ЄС.



Варто зазначити, що регулювання штучного інтелекту в ЄС здійснюється не лише через AI act, а й через ширший масив нормативно-правових актів. Крім того, існують етичні настанови щодо створення, впровадження та використання надійного ШІ – зокрема, Етичний кодекс ШІ (Ethics Guidelines for Trustworthy AI). Низка актів перебуває на стадії розробки або оновлення, серед них –

Директива про відповідальність за дефектну продукцію (Product Liability Directive), Директива про відповідальність за шкоду, заподіяну ШІ (Artificial Intelligence Liability Directive). Нижче представлено інші ключові нормативно-правові акти ЄС у сфері регулювання ШІ, при цьому слід врахувати, що цей перелік не є вичерпним.



Необхідність такого концептуального огляду законодавства ЄС у сфері регулювання ШІ зумовлена тим, що, як зазначено в офіційних документах Міністерства цифрової трансформації України (далі - Мінцифри) : «Рано чи пізно Україна повинна буде імплементувати AI act Європейського Союзу як одну з умов євроінтеграції в цифровій сфері»⁸⁷.

Хоча в Україні, як і в більшості країн світу, ще не прийнято спеціалізованого нормативно-правового акту, який би комплексно регулював сферу штучного інтелекту, держава активно працює над формуванням

⁸⁷ Дорожня карта з врегулювання штучного інтелекту в Україні. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf (дата звернення: 31.03.2025).

відповідного правового поля. Так, було прийнято Концепцію розвитку штучного інтелекту в Україні⁸⁸, Стратегію цифрового розвитку інновацій до 2030 року⁸⁹, розроблено Дорожню карту з врегулювання штучного інтелекту в Україні⁹⁰, видано методичний матеріал «Права людини в епоху штучного інтелекту. Виклики та правове регулювання»⁹¹, «Поради з відповідального використання штучного інтелекту публічними службовцями»⁹², «Рекомендації щодо відповідального використання ШІ: питання права інтелектуальної власності»⁹³ та ін.

Власне, Дорожня карта становить особливий інтерес, оскільки в ній передбачені конкретні подальші кроки України на шляху імплементації AI Act. З огляду на це, з метою уникнення дублювання змісту, пропонується ознайомитися з документом за допомогою гіперпосилання.



ПЕРЕВІРКА ЗНАНЬ

What is true and what is false?

Justify your answer.

1. Система Verdictum PRO в Україні використовується з метою прогнозування рішення суду.

⁸⁸ Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#n35> (дата звернення: 31.03.2025).

⁸⁹ WINWIN: Україна затвердила Стратегію цифрового розвитку інновацій до 2030 року [Електронний ресурс] // Міністерство цифрової трансформації України. – Режим доступу: <https://thedigital.gov.ua/news/winwin-ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-innovatsiy-do-2030-roku> (дата звернення: 31.03.2025).

⁹⁰ Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf (дата звернення: 31.03.2025).

⁹¹ Права людини в епоху штучного інтелекту. Виклики та правове регулювання. URL: <https://drive.google.com/file/d/1YLb1X8wCMQI3g8LjPsERa2b58GM1fRS2/view> (дата звернення: 31.03.2025).

⁹² Поради з відповідального використання штучного інтелекту публічними службовцями. URL: https://drive.google.com/file/d/15_85zVEXz_y2IFDNXfMJTwM9IEeX6mF/view (дата звернення: 31.03.2025).

⁹³ Рекомендації щодо відповідального використання ШІ: питання права інтелектуальної власності. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Рекомендації_щодо_ШІ_та_інтелектуальної_власності.pdf (дата звернення: 31.03.2025).

2. AI Act Європейського Союзу встановлює обов'язкове регулювання для всіх систем ШІ.
3. Системи ШІ високого ризику відповідно до AI Act повинні бути зареєстровані в спеціальній базі даних ЄС.
4. ChatGPT є прикладом системи генеративного ШІ, що використовує машинне навчання.
5. COMPAS – це система прогнозування судових рішень, яка широко використовується в США і визнана об'єктивним помічником у діяльності суддів.
6. Машинне навчання – це підхід, за якого алгоритм самостійно навчається на основі даних.
7. Використання ШІ в юридичній діяльності значно спрощує роботу юриста, забезпечуючи економію часу та відсутність потреби у людському нагляді.
8. Системи ШІ, які генерують deepfake-контент, належать до категорії високого ризику відповідно до AI Act Європейського Союзу.
9. Ігри та фільтри в соцмережах належать до систем ШІ загального ризику відповідно до AI Act.
10. AI Act вимагає, щоб будь-який контент, створений ШІ (наприклад, текст чи зображення), був промаркований відповідним чином.
11. Право людини отримати пояснення щодо того, як було ухвалене рішення не стосується автоматизованого рішення згідно з GDPR.
12. Україна вже прийняла Дорожню карту з врегулювання штучного інтелекту, яка передбачає імплементацію AI Act.

ЗАВДАННЯ



1. Legal Case Analysis (Loomis v. Wisconsin, 2016)

Проаналізуйте справу COMPAS – алгоритм оцінки ризику рецидиву в США (Loomis v. Wisconsin, 2016).

Questions:

- Чи було порушено право на справедливий суд?
- Як забезпечити прозорість алгоритмів у кримінальному судочинстві?
- Який підхід можна запропонувати для країн ЄС чи України?



2. Reflection «Artificial Intelligence as a Judge: Science Fiction or the Future of Justice?»

Підготуйте есе-доповідь, в якій потрібно оцінити потенціал і ризики використання ШІ у винесенні судових рішень.



3. Parliamentary Debate Simulation

Уряд пропонує законопроект, який дозволяє використання ШІ для автоматичного виявлення податкових правопорушень.

Підготуйте у групах міні-дебати з правовими, етичними та соціальними аргументами.



4. Ethical Audit

Муніципалітет запровадив ШІ для розпізнавання облич у публічних місцях з метою безпеки.

Проведіть правово-етичний аудит цієї ініціативи за моделлю ЄС (законність, необхідність, пропорційність, етичність, прозорість).

Розділ VII ПРАВОВІ ТЕХНОЛОГІЇ

LEGALTECH

1. Цифровізація юридичних послуг: проблематика дефініцій у контексті LegalTech та суміжних понять

Одним із провідних напрямів трансформації правничих послуг у XXI столітті є впровадження цифрових технологій у сфері права, що у науковій та професійній літературі позначається терміном **LegalTech**. Незважаючи на значне поширення цього поняття у фаховому



дискурсі, його зміст залишається концептуально нечітким. Однією з причин такої термінологічної розмитості є наявність низки близьких за змістом понять, зокрема **RegTech**, **SmartLaw**, **LawTech** та **Digital Law**, які, залежно від контексту, можуть трактуватися як синонімічні або такі, що позначають суміжні, але не тотожні явища. Наразі у правовій доктрині та практиці відсутні усталені дефініції зазначених термінів, що призводить до варіативного їх використання.

У зв'язку з цим актуальним є здійснення стислого порівняльного аналізу наведених понять з метою виявлення їхніх сутнісних ознак і визначення співвідношення між ними в контексті цифровізації правничої діяльності.

LegalTech (від **Legal Technology**) – це сукупність цифрових технологій, програмних рішень та інноваційних підходів, спрямованих на оптимізацію, автоматизацію або підвищення ефективності надання юридичних послуг. Зміст цього поняття охоплює як інструменти для правників (наприклад, системи управління кейсами, аналіз судової практики, генератори договорів), так і інноваційні платформи для комунікації з клієнтами.

На сучасному етапі більшість LegalTech-рішень розробляються стартапами, метою яких є модернізація традиційного правничого ринку, подолання його інерційності та відкритість до інновацій. Водночас, LegalTech не обмежується

лише автоматизацією – його сутність полягає у переосмисленні моделі юридичної допомоги в умовах цифрової трансформації суспільства⁹⁴.

LegalTech-технології часто базуються на елементах штучного інтелекту (ШІ), включаючи алгоритми машинного навчання, обробку природної мови, прогнозувальну аналітику тощо. Однак важливо розмежовувати ці два поняття: ШІ є ширшим феноменом, який охоплює всі сфери людської діяльності, не лише юридичну.

RegTech (Regulatory Technology) – це окрема категорія цифрових рішень, орієнтованих на забезпечення відповідності нормативно-правовим вимогам, передусім у фінансовому секторі. Застосування RegTech стосується таких процесів, як регуляторний комплаєнс, внутрішній аудит, управління ризиками, боротьба з відмиванням доходів, автоматизована звітність та ін.

Комплаєнс (від англ. *compliance* – «відповідність», «дотримання») у правовому та корпоративному контексті означає діяльність, спрямовану на забезпечення відповідності компанії вимогам законодавства, внутрішнім політикам, етичним стандартам та іншим нормативним актам.

RegTech має тісний зв'язок із LegalTech, однак його предметне поле є більш спеціалізованим та регулюється переважно міжнародними стандартами фінансового нагляду.

Термін **SmartLaw** не має усталеного дефінітивного статусу в юридичній науці, однак у прикладній площині його часто вживають для позначення інтерактивних платформ або «конструкторів» юридичних документів⁹⁵. Ці системи дозволяють формувати персоналізовані договори,



⁹⁴ Taher Abou-eleid. The future of Legal Technology How will legal technology change the legal practice? July 2022. URL: https://www.researchgate.net/publication/361722506_The_future_of_Legal_Technology_How_will_legal_technology_change_the_legal_practice (date of access 28.04.2025).

⁹⁵ Unsere Rechtsdokumente auf einen Blick. URL: <https://www.smartlaw.de/rechtsdokumente> (date of access 28.04.2025).

позовні заяви чи інші документи без участі юриста, що підвищує доступність базової правової допомоги.

LawTech зазвичай вживається в Європі для позначення технологій, які безпосередньо покращують доступ до правосуддя. Існує також окрема думка, що LawTech-фокус робиться на самообслуговуванні, демократизації доступу до правових знань (юридичні боти, конструктори юридичних документів, онлайн-консультанти тощо). У той час як LegalTech переважно орієнтований на оптимізацію професійної діяльності юристів⁹⁶.

Digital Law – це новий міждисциплінарний напрям права, що досліджує та регулює суспільні відносини на перетині цифрових технологій і правових норм. До сфери Digital Law належать питання захисту персональних даних, кібербезпеки, регулювання штучного інтелекту, електронної ідентифікації, цифрового контенту, прав у метавсесвітах тощо. Цей напрям права динамічно розвивається під впливом цифрової трансформації державного управління, бізнесу та повсякденного життя.

Оскільки термін LegalTech є найбільш поширеним у міжнародному науковому та практичному дискурсі, у подальшому використовуватиметься саме ця назва.

2. LegalTech: значення, переваги та виклики

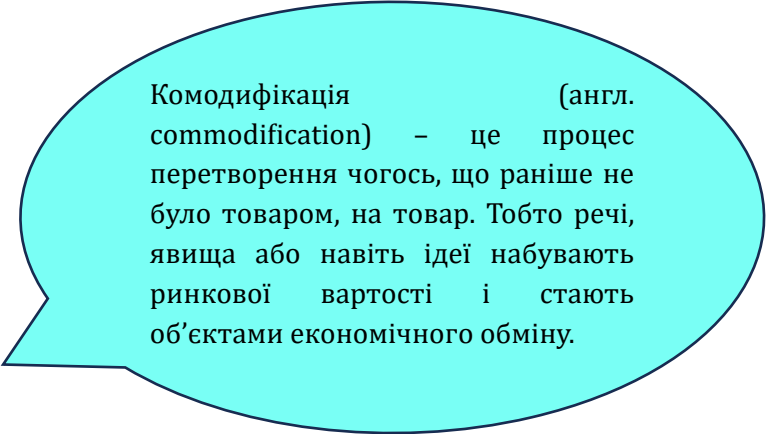
Юридичні інновації мають вагоме значення для практикуючого юриста, оскільки вони підвищують його ефективність та продуктивність, а також здатні забезпечувати інформацією, необхідною для планування майбутньої стратегії.

Технології у праві дозволяють досягнути наступних цілей:

⁹⁶ Prabhjot Singh. Legal Tech and Law Tech- Understand the Difference. URL: <https://www.linkedin.com/pulse/difference-between-legal-tech-law-prabhjot-singh/> (date of access 28.04.2025).

- **Географічна**

доступність. Технології допомогли юридичним фірмам вийти на міжнародний рівень. Комодифікація деяких юридичних послуг дозволила надавати їх транснаціонально.



Комодифікація (англ. commodification) – це процес перетворення чогось, що раніше не було товаром, на товар. Тобто речі, явища або навіть ідеї набувають ринкової вартості і стають об'єктами економічного обміну.

Наприклад, коли договірне право подібне в різних юрисдикціях, клієнт може обрати країну зі списку і завантажити відповідний шаблон договору. Ті юридичні фірми, що впроваджують технології, розширюють свій ринок, а технології стимулюють їхнє зростання.

- **Краща прозорість.** Юридичні технології зробили прозорішою раніше закриту систему. Клієнти тепер можуть бачити стан справ, витрати та іншу релевантну інформацію. Такий орієнтований на клієнта підхід позитивно впливає на галузь.

- **Раціональніше використання людських ресурсів та інклюзивність.** Завдяки технологіям вони можуть бути переорієнтовані на завдання з більшим впливом — наприклад, параюристи можуть займатися юридичними дослідженнями чи відвідувати судові засідання, замість монотонного управління документами.

- **Швидше виконання завдань та управління часом.** За правильного використання технології працюють швидше і ефективніше, ніж найкращі спеціалісти. Рішення на базі ШІ можуть шукати інформацію та аналізувати документи за мілісекунди, тоді як раніше це займало години чи навіть дні⁹⁷.

Хоч LegalTech створює нові можливості для юристів і громадян, його використання несе і низку ризиків. Вони стосуються не лише технічних помилок, а й фундаментальних засад правової держави: справедливості, права на захист,

⁹⁷ Taher Abou-eleid. The future of Legal Technology How will legal technology change the legal practice? July 2022. URL: https://www.researchgate.net/publication/361722506_The_future_of_Legal_Technology_How_will_legal_technology_change_the_legal_practice (date of access 28.04.2025).

прозорості та недискримінації. Нижче наведено ключові ризики притаманні використанню LegalTech.

1. Ризик допущення помилок системою.

З одного боку, застосування технологій LegalTech дозволяє зменшити кількість помилок, викликаних людським фактором. Проте слід враховувати, що і самі системи можуть допускати помилки. Це може статися через неповноту або неякісність даних, на яких моделі навчалися, а також через феномен так званої «чорної скриньки» (black box), коли внутрішні механізми ухвалення рішень залишаються непрозорими навіть для розробників. У зв'язку з цим результати роботи LegalTech-рішень завжди повинні підлягати ретельній перевірці та юридичній оцінці фахівцем.

Ілюстративним прикладом є справа *Faridian v. DoNotPay, Inc.* (Case No. CGC-23-604987)⁹⁸, подана у США в 2023 році. Позивач стверджував, що отримані через платформу DoNotPay юридичні послуги були неналежної якості, а наслідки використання автоматизованої системи виявилися несприятливими через «машинну недбалість».

2. Непрозорість алгоритмів (ефект «чорної скриньки»).

Однією з ключових проблем використання технологій штучного інтелекту у сфері LegalTech є їхня непрозорість. У більшості випадків користувачі не мають



можливості з'ясувати, на основі яких критеріїв або міркувань система прийняла те чи інше рішення. Багато LegalTech-інструментів, що використовують алгоритми машинного навчання, не надають пояснень щодо логіки або обґрунтувань своїх висновків.

Відсутність так званого «права на пояснення» (right to explanation) суттєво обмежує права особи на юридичний захист. Якщо користувач або сторона

⁹⁸ Faridian v. DoNotPay, Inc. Class Action Complaint. Case No. CGC-23-604987. Superior Court of California, County of San Francisco. 2023. URL: <https://www.classaction.org/media/faridian-v-donotpay-inc.pdf> (date of access 28.04.2025).

процесу не розуміє, на яких підставах було ухвалено рішення, він позбавляється можливості ефективно оскаржувати або захищати свої права, оскільки невідомо, на які аргументи потрібно апелювати.

3. Дискримінація та упередженість у даних.

Технології LegalTech базуються на алгоритмах штучного інтелекту, які навчаються на великих масивах даних. Проте якщо вихідні дані містять упередженість або дискримінаційні патерни, то і результати роботи системи можуть відтворювати або навіть посилювати ці недоліки. У випадках, коли навчальні дані відображають історичні рішення із виявами дискримінації, автоматизовані рекомендації LegalTech-рішень можуть стати неетичними або суперечити законодавству.

Ілюстративним прикладом є ситуація з компанією Amazon у 2018 році (помилка часто асоціюється з 2017 роком, але офіційно проблему виявили та розголосили у 2018 році). Компанія припинила використання внутрішньої системи штучного інтелекту для найму персоналу після того, як виявилось, що алгоритм систематично занижував оцінку резюме жінок. Причиною стало те, що система навчалася на даних про успішні резюме попередніх років, де домінували чоловіки.

4. Недотримання конфіденційності, безпеки та захисту даних.

LegalTech-рішення працюють із великими обсягами чутливої юридичної інформації, зокрема з персональними даними клієнтів, деталями договорів та іншими конфіденційними матеріалами. Прогалини у захисті таких даних можуть призвести до серйозних наслідків, зокрема:

- витоків персональних даних;
- використання персональної інформації не за призначенням;
- порушення адвокатської таємниці.

Додатковим ризиком є те, що у багатьох випадках дані, введені користувачами в LegalTech-платформи, зберігаються на серверах розробників або сторонніх постачальників послуг, що посилює загрозу несанкціонованого доступу.

Показовим прикладом є ситуація у Франції у 2019 році: Національна рада адвокатів Франції (Conseil National des Barreaux, CNB) подала кримінальну скаргу до прокуратури Парижа проти юридичної платформи *Doctrine.fr*. Платформу звинувачували у масовому зборі, збереженні та публікації судових рішень без належної згоди сторін, що, на думку скаржників, могло призвести до порушення професійної таємниці, конфіденційності юридичної інформації та незаконного використання персональних даних адвокатів⁹⁹.

5. Обмежений доступ для вразливих груп населення.

Більшість рішень у сфері LegalTech функціонують на комерційній основі, що створює фінансові бар'єри для вразливих груп населення. Вартість підписки, консультацій або використання платформ може бути надто високою для осіб з обмеженими фінансовими можливостями.

Окрім фінансових обмежень, існують також технологічні та освітні бар'єри. Для ефективного використання LegalTech необхідні доступ до інтернету, наявність відповідних пристроїв (смартфонів, комп'ютерів) та певний рівень цифрової грамотності. Це становить додаткові труднощі для осіб похилого віку, людей з інвалідністю, внутрішньо переміщених осіб та інших соціально вразливих категорій. Таким чином, розширення LegalTech без урахування принципу доступності може призводити до ще більшої юридичної нерівності.

6. Етична дилема: сервіс чи професія?

Розвиток LegalTech стирає традиційну межу між наданням правової допомоги як професійною діяльністю і як комерційним сервісом. Це породжує фундаментальне питання: чи можливо

ETHICAL DILEMMA:



⁹⁹ Conseil national des barreaux. Le CNB et le barreau de Paris ont déposé une plainte pénale contre Doctrine.fr. URL: <https://www.cnb.avocat.fr/fr/actualites/le-cnb-et-le-barreau-de-paris-ont-depose-une-plainte-penale-contre-doctrinefr> (date of access 28.04.2025).

повністю автоматизувати право, чи, навпаки, кожен етап юридичних послуг вимагає етичної рефлексії фахівця?

Діяльність адвоката в Україні згідно з Правилами адвокатської етики передбачає не лише знання норм права, а й здатність оцінювати ситуацію комплексно, обов'язок адвоката «виходити з інтересів клієнта» (ст.8), «діяти добросовісно з урахуванням наслідків своїх дій для клієнта» (ст.11)¹⁰⁰.

Наразі ж Legal Bots та автоматизовані платформи не здатні гарантувати врахування етичних аспектів, адже діють виключно в межах запрограмованих алгоритмів і не володіють можливістю самостійного морального оцінювання або індивідуалізації підходу до справи. Це ставить під сумнів можливість повної автоматизації юридичної професії.



¹⁰⁰ Правила адвокатської етики : затв. з'їздом адвокатів України 9 червня 2017 р. (зі змінами та доповненнями) // Національна асоціація адвокатів України. URL: <https://zakon.rada.gov.ua/rada/show/n0001891-17#Text> (дата звернення: 26.04.2025).

3. Типологія технологій LegalTech

Широка представленість та різноманітність інструментів LegalTech зумовили появу численних спроб їх класифікації, спрямованих на поглиблене розуміння їхньої сутності та ролі в трансформації правничої діяльності. Так, суддя Апеляційного суду Каїру (Єгипет) Taher Abou-eleid, він же ж дослідник юридичних технологій, у своєму науковому дослідженні здійснив спробу об'єднати існуючі класифікації технологій LegalTech. Він наводить наступні три види класифікацій.

Перша. Згідно з дослідженням *Bucerius Law School* (Німеччина) та *Boston Consulting Group* (США), виокремлено три основні типи юридичних технологій:

1. Технології розширення можливостей (Empowerment technologies): ці технології пов'язані з цифровізацією юридичних даних.
2. Рішення для підтримки операційної діяльності (Support Operations Solutions): включають рішення для бек-офісної роботи, бухгалтерського обліку, розвитку бізнесу, управління людськими ресурсами, ведення справ і документообігу.
3. Технології матеріального (субстантивного) права (Technology of substantive law): якщо перші два типи стосуються адміністративних питань, то ця група технологій спрямована саме на надання рішень у сфері матеріального права, судового розгляду, аналізу справ.

Друга. У базі даних *Stanford Legal Codex* (США) виокремлено дев'ять типів юридичних технологій, серед яких: автоматизація документів, управління юридичною практикою, юридичні дослідження, юридична освіта та онлайн-врегулювання спорів.

Третя. *Zoë Andrae*, керуюча директорка компанії *Lecare* у Гамбурзі (Німеччина), яка (*Lecare*) вже понад 30 років виробляє веб-програмні рішення для юридичних відділів та юридичних фірмСЕО і спеціалізується на юридичних

технорішеннях, виокремлює п'ять категорій юридичних технологій для стартапів у межах правової системи:

1. Правові рішення (Law solutions): це сервіси типу «зроби сам» – наприклад, платформи для складання документів, де користувачі можуть укладати прості договори, заповіти, документи про розлучення тощо. До цієї категорії також належать смарт-контракти на базі блокчейн-технологій.

2. Онлайн-юридичні маркетплейси, мережі та багатфункціональні платформи: ці технології з'єднують юристів із клієнтами. Прикладами таких порталів є сервіси з надання юридичних консультацій, платформи юридичних послуг і бази юридичних даних.

3. Високотехнологічні інструменти для окремих видів юридичних послуг: до них належать технології для перевірки документів, електронного розкриття доказів, управління об'єктами інтелектуальної власності, автоматизованого збору документів, управління юридичними контрактами, аналітики юридичних досліджень, управління юридичною практикою.

4. Платформи з системами онлайн-врегулювання спорів, які докорінно змінюють юридичну професію.

5. Юридичні системи штучного інтелекту (AI): найкращий приклад – ROSS, програма штучного інтелекту на базі технології IBM Watson, яка допомагає тисячам юристів у США працювати швидше та ефективніше¹⁰¹.

Таким чином, розмаїття підходів до типологізації технологій LegalTech свідчить про багатовимірність цієї сфери та її стрімку еволюцію. Виявлені класифікації дозволяють краще зрозуміти особливості правничих технологій, їх функціональне призначення та вплив на трансформацію юридичної діяльності. Водночас така типологізація відкриває нові потенційні напрями професійної діяльності для юристів, формуючи запит на спеціалізації у сфері цифрових правових послуг.

¹⁰¹ Taher Abou-eleid. The future of Legal Technology How will legal technology change the legal practice? July 2022. URL: https://www.researchgate.net/publication/361722506_The_future_of_Legal_Technology_How_will_legal_technology_change_the_legal_practice (date of access 28.04.2025).

4. Сучасні технології LegalTech: основні приклади

Варто зазначити, що інструменти LegalTech розробляються з орієнтацією або на міжнародне право, або на національні правові системи окремих держав, оскільки між країнами існують істотні відмінності у правовому регулюванні. Відповідно, набір LegalTech-інструментів у кожній юрисдикції формується з урахуванням особливостей її правового середовища.

Німеччина. В Німеччині існує кілька компаній у сфері LegalTech. Деякі з них є невеликими та вузькоспеціалізованими, інші ж пропонують рішення для широкої аудиторії. До останніх належать, зокрема, такі компанії:

- **flightright**¹⁰²: компанія спеціалізується на компенсаціях авіапасажирам. У разі затримок чи скасування рейсів клієнти часто мають право на відшкодування, але процес його отримання зазвичай є складним або дорогим. Через flightright користувачі можуть легко подати свої вимоги. Оплата здійснюється лише у разі успіху – як відсоткова комісія від отриманої суми.
- **smartlaw**¹⁰³: це інструмент, за допомогою якого компанії та приватні особи можуть самостійно створювати документи, наприклад, договори або заяви на звільнення.
- **advocado**¹⁰⁴: портал для консультування, який, зокрема, сполучає приватних осіб з юристами. Клієнти отримують безкоштовну попередню оцінку свого випадку. Якщо вони хочуть подальшої юридичної допомоги або представництва, їм пропонують фіксовану вартість послуги.
- **CONNY**¹⁰⁵ (раніше [wenigermiete.de](https://www.wenigermiete.de/)): зниження орендної плати можливе з багатьох причин. CONNY – це платформа, яка допомагає споживачам домогтися таких знижень без зайвих складнощів. Як і в інших подібних сервісах, оплата відбувається лише у разі виграшу справи.

¹⁰² Flightright. URL: <https://www.flightright.de/> (date of access 28.04.2025).

¹⁰³ Smartlaw. URL: <https://www.smartlaw.de/> (date of access 28.04.2025).

¹⁰⁴ Advocado. URL: <https://www.advocado.de/> (date of access 28.04.2025).

¹⁰⁵ CONNY. URL: <https://conny.de/> (date of access 28.04.2025).

- **geblitzt.de**¹⁰⁶: також працює на умовах оплати за результат. Компанія перевіряє штрафи, заборони на водіння та нараховані штрафні бали (наприклад, за порушення ПДР)¹⁰⁷.

США. Ця країна відома широкому сприянню розвитку штучного інтелекту та юридичних технологій. У США зареєстровано найбільшу кількість Legal Tech-компаній у світі, серед яких відомі такі Legal Tech інструменти, як FiscalNote, Harvey AI, Rocket Lawyer, Casetext, Everlaw та ін. Американський ринок юридичних технологій охоплює різноманітні напрями – від автоматизації документів та електронного розкриття доказів до платформ онлайн-консультацій та інтелектуальних систем аналізу судової практики.

CoCounsel (Casetext)¹⁰⁸ позиціонується як юридичний помічник на базі штучного інтелекту, який здатний виконувати, зокрема, наступні завдання: вилучати потрібну конкретну інформацію з великого обсягу матеріалів, генерувати хронологію подій з наданих матеріалів, формулювати правильні запитання для свідка, резюмувати, аналізувати контракти на відповідність політики компанії та ін. Даний інструмент розроблений для правової системи США, однак власники компанії планують розширити його діяльність також на Австралію та Канаду.

Harvey AI¹⁰⁹ – юридичний на базі ШІ, але орієнтований здебільшого на роботу корпоративних юристів (натомість CoCounsel (Casetext) – здебільшого на судову діяльність) та призначений автоматизовувати документообіг, створювати контракти, аналізувати дані, проводити юридичні дослідження та ін. До того ж, Harvey AI інтегрований з багатьма іншими корпоративними платформами, завдяки чому має розширену функціональність. Використовує більш як 50 мов, тому здатний працювати в різних країнах та правових системах.

¹⁰⁶ Geblitzt.de. URL: <https://www.geblitzt.de/> (date of access 28.04.2025).

¹⁰⁷ TalentRocket. Was ist eigentlich Legal Tech? URL: <https://www.talentrocket.de/karrieremagazin/details/was-ist-eigentlich-legal-tech> (date of access 28.04.2025).

¹⁰⁸ Casetext CoCounsel. URL: <https://casetext.com/cocounsel> (date of access 28.04.2025).

¹⁰⁹ Harvey. URL: <https://www.harvey.ai> (date of access 28.04.2025).

FiscalNote¹¹⁰ – за його допомогою можна не просто відстежувати законодавчі зміни з конкретного питання, а й законодавчу політику щодо нього: кому належала ініціатива, стенограми комітетів, як голосували партії, хронологію розвитку вирішення відповідних питань, аналітику відповідної політики та ін.

Everlaw¹¹¹ – призначена для пріоритизації та класифікації документів, огляду документів за допомогою штучного інтелекту для швидкого визначення релевантної інформації, розширеного пошуку і фільтрацію. Також вона включає інструменти для редагування, анотування та коментування документів, візуалізацію хронології справи, автоматизовану транскрипцію аудіо- та відеофайлів для прискореного перегляду, а також функціонал для командної співпраці через спільне тегування, анотації та обмін документами.

Rocket Lawyer¹¹² Це американська платформа юридичних онлайн-послуг, яка надає фізичним особам та малому і середньому бізнесу можливість створювати персоналізовані юридичні документи, підписувати їх електронним підписом, реєструвати бізнес, формувати плани нерухомості та здійснювати перегляд юридичних документів. Компанія також пропонує мережу адвокатів для консультацій зі споживачами та представниками малого бізнесу через власну сервісну платформу.

Україна. В Україні ринок LegalTech, попри відносну новизну, демонструє швидкі темпи зростання та, за оцінками, може досягти обсягу в 100 мільйонів доларів США до 2025 року. Подальший розвиток галузі потребує вдосконалення правового регулювання штучного інтелекту, підвищення довіри до онлайн-послуг, адаптації юридичної професії до нових умов та забезпечення належного фінансування інновацій.

Станом на 2024 рік в Україні функціонує близько 65 LegalTech – продуктів, орієнтованих переважно на бізнес та громадян, із фокусом на автоматизацію створення документів і аналіз даних з реєстрів. Традиційні юридичні компанії

¹¹⁰ FiscalNote. URL: <https://fiscalnote.com> (date of access 28.04.2025).

¹¹¹ Everlaw. URL: <https://www.everlaw.com/> (date of access 28.04.2025).

¹¹² Rocket Lawyer. URL: <https://www.rocketlawyer.com/> (date of access 28.04.2025).

активно співпрацюють із технологічним сектором, розробляючи власні рішення або сприяючи розробці сервісів, частину яких експортують за кордон.

Унаслідок повномасштабної війни у 2022–2023 роках ринок зазнав тимчасового спаду, у зв'язку з переорієнтуванням на DefenseTech. Однак з другої половини 2023 року спостерігається поступове відновлення¹¹³.

Задля натхнення та мотивації доцільно навести приклад успішного українського LegalTech-стартапу, а саме, компанію **AXDRAFT**. Вона була заснована у 2017 році в Києві братами Юрієм Зарембою (юрист, який працював в юридичній фірмі) та Олегом Зарембою (програміст). Ідея створення стартапу виникла внаслідок усвідомлення Юрієм масштабів рутинної роботи, з якою щодня стикаються юристи. Це спонукало його до об'єднання зусиль зі своїм братом та до розробки інструменту для автоматизації юридичної роботи.

AXDRAFT спеціалізується на автоматизації процесу створення юридичних документів та управлінні життєвим циклом контрактів (Contract Lifecycle Management, CLM). Платформа дозволяє значно скоротити час на підготовку документів: у середньому створення, редагування, погодження та підписання документа займає 4–5 хвилин, що приблизно вдесятеро швидше порівняно з традиційними методами.

У грудні 2020 року компанія була придбана американською корпорацією Onit, Inc., одним із провідних постачальників рішень для автоматизації юридичних процесів і застосування штучного інтелекту в корпоративному управлінні.

Технологічна основа AXDRAFT базується на алгоритмах, що перетворюють процес складання документів на формат інтерактивних запитань і відповідей (Q&A), а також забезпечують інтеграцію з внутрішніми базами даних, підтримку електронного підпису та багатомовність, включно з підтримкою китайської та японської мов.

¹¹³ Український Legal Tech: стартапи та вплив AI. *Mezha.Media*. URL: <https://mezha.media/articles/ukrainskyy-legal-tech-startupy-ta-vplyv-ai/> (дата звернення: 26.04.2025).

AXDRAFT є прикладом успішної української технологічної ініціативи, що досягла міжнародного визнання та інтегрувалася у світову LegalTech-екосистему.

З метою уникнення дублювання інформації пропонується детальніше ознайомитися з іншими 65 наявними Legal Tech-інструментами та стартапами в Україні за наданим інтерактивним посиланням¹¹⁴. В ньому наведено короткі описи інструментів, вказано цільову аудиторію, види наданих послуг, а також розміщено посилання на офіційні вебсторінки проєктів.



1	Airlaw Pro
2	Legal Nodes
3	AxDraft
4	Liga
5	Monitor.Estate
6	Бабуся від OpenDataBot
7	OpenDataBot
8	Protocol
9	ПравоМен
10	Автоматизації внутрішній процесі...
11	«Oblava bot»

5. Правове регулювання LegalTech: міжнародний досвід

Правове регулювання сфери LegalTech на глобальному рівні перебуває на початковій стадії розвитку. Наразі відсутні усталені підходи та єдине розуміння щодо врегулювання відповідних правовідносин. У зв'язку з цим перші кроки, що здійснюються державами у напрямі правового оформлення LegalTech, суттєво різняться за змістом і формою.



США. Цікавим фактом є те, що у 2012 році Американська асоціація адвокатів (American Bar Association, ABA) внесла зміни до Model Rules of Professional Conduct (Модельних правил професійної етики), включивши до вимог для адвокатів базове розуміння «technology competence» (технологічної компетентності). Зокрема, у Коментарі 8 до Правила 1.1 (Competence) було додано, що адвокат повинен «йти в ногу зі змінами у законодавстві та практиці,

¹¹⁴ Legal Tech інструменти та стартапи в Україні. *Airtable*. URL: <https://airtable.com/appKMTdPDQzj59Xca/shrYd4scz7tr8kuHD/tblk6Fk8ozCYld3fV> (дата звернення: 26.04.2025).

включаючи переваги й ризики, пов'язані з відповідними технологіями»¹¹⁵. Тому необізнаність у LegalTech може розцінюватись навіть як порушення професійної етики.

Водночас єдиного правового регулювання самих технологій в США немає, а політика щодо його регулювання відзначається суперечністю. Так, у 2023 році президент США Джо Байден видав указ, спрямований на мінімізацію ризиків для суспільства внаслідок використання ШІ. В указі йшлося про встановлення нових стандартів безпеки ШІ, захист конфіденційності, дотримання принципів справедливості та громадянських прав, гарантування прав споживачів і працівників, стимулювання інновацій та конкуренції¹¹⁶. Однак, 20 січня 2025 року, одразу після інавгурації новий президент США Дональд Трамп відкликав відповідний указ¹¹⁷, що мало значні наслідки для американського суспільства в цілому. Адже, фактично наразі різні штати США ухвалюють власні закони щодо, наприклад, конфіденційності даних, модерації контенту, штучного інтелекту тощо. Це ускладнює діяльність технологічних компаній, які змушені одночасно дотримуватися різних, а іноді й суперечливих, вимог¹¹⁸.

Така політика призвела до того, що провідні технологічні компанії, об'єднавшись (зокрема, Google, Meta, OpenAI, Business Roundtable та ін.), активно лобіюють федеральну владу щодо прийняття єдиного загальнонаціонального закону, який би усунув фрагментованість і скасував дію окремих штатних актів у сфері штучного інтелекту та цифрових сервісів. Вони прямо закликають до *federal preemption* – пріоритету федерального закону над штатними для спрощення юридичного обслуговування та зменшення регуляторних бар'єрів¹¹⁹.

¹¹⁵ Lawyers and Technological Competence. *Thomson Reuters*. URL: <https://www.thomsonreuters.com/en-us/posts/legal/lawyers-technological-competence/> (date of access 28.04.2025).

¹¹⁶ Красніков Денис. Новий указ Президента Байдена про штучний інтелект: більше обмежень чи стимулювання розвитку. URL: <https://www.ukrinform.ua/rubric-technology/3787099-novij-ukaz-prezidenta-bajdena-pro-stucnij-intelekt-bilse-obmezen-ci-stimuluvanna-rozvitku.html> (дата звернення: 28.04.2025).

¹¹⁷ Shepardson David. Trump revokes Biden executive order on addressing AI risks. January 21, 2025 URL: <https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/> (date of access 28.04.2025).

¹¹⁸ States Navigating Tech Legislation in 2024. CCIA. URL: <https://ccianet.org/articles/states-navigating-tech-legislation-2024/> (date of access 28.04.2025).

¹¹⁹ Shaping the AI Action Plan: Responses to the White House's Request for Information. Just Security. URL: <https://www.justsecurity.org/109203/us-ai-action-plan/> (date of access 28.04.2025).

Судова практика США у зазначеному аспекті також є показовою. Зокрема, у справі **Upsolve Inc. v. James** (2022)¹²⁰ федеральний суд у Нью-Йорку ухвалив рішення на користь неприбуткової організації **Upsolve**, яка розробила програму для навчання неюрислів надання безоплатної правової допомоги малозабезпеченим мешканцям Нью-Йорка у справах про стягнення боргів.

Суд дійшов висновку, що застосування положень про заборону неюрислам надавати юридичні поради (UPL rules) у цьому вузько визначеному контексті порушує положення Першої поправки до Конституції США, що гарантує свободу слова, оскільки діяльність Upsolve полягала саме у наданні юридичних порад, а не лише в поширенні загальної інформації.

У межах розгляду суд надав попередню судову заборону (*preliminary injunction*), яка дозволила Upsolve реалізовувати свою програму без ризику притягнення до відповідальності за несанкціоновану юридичну практику. При цьому було наголошено, що рішення стосується виключно даного інструменту LegalTech¹²¹.

Якщо в попередній справі сама компанія спрацювала на випередження і подала позов до суду, щоб фактично визнати законною свою діяльність та унеможливити позов прокуратури з приводу своєї діяльності, то в наступній справі все навпаки. Популярну компанію DoNotPay, яка позиціонує себе як «перший у світі робот-юрист» звинуватили (вище згадувана справа Faridian v. DoNotPay, 2023 у штаті Каліфорнія) в наданні юридичних послуг без відповідної ліцензії, що порушує положення законодавства штату Каліфорнія (California State Bar Act), а також в оманливій рекламі, обіцяючи можливість «найняти юриста одним кліком» без фактичного залучення ліцензованих фахівців.

Крім того, до компанії були висунуті претензії щодо низької якості наданих документів, які містили суттєві помилки та неточності. Позов був поданий із вимогою визнати діяльність DoNotPay незаконною, заборонити надання

¹²⁰ U.S. Court of Appeals for the Second Circuit, Case No. 22-1345.

CourtListener. URL: <https://www.courtlistener.com/docket/66910999/upsolve-inc-v-james/> (accessed 29 Apr. 2025).

¹²¹ First Amendment Protects Non-Lawyers in Providing Legal Advice in Debt Cases, Federal Court Rules. *LawNext*. URL: <https://www.lawnext.com/2022/05/first-amendment-protects-non-lawyers-in-providing-legal-advice-in-debt-cases-federal-court-rules.html> (date of access 28.04.2025).

юридичних послуг без ліцензії, відшкодувати кошти споживачам та припинити недобросовісну конкуренцію.

У червні 2024 року сторони повідомили суд про досягнення попередньої мирової угоди. Деталі угоди не розголошувались¹²². Ця справа є знаковою, оскільки підкреслює потенційні ризики для споживачів при використанні автоматизованих юридичних сервісів та демонструє готовність судів США оцінювати правовий статус діяльності таких платформ.



Німеччина. Примітно, що в Німеччині у жовтні 2021 року було прийнято так званий Закон про LegalTech (офіційна назва — *Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt*, або «Закон про сприяння споживчо-орієнтованим пропозиціям на ринку правових послуг»)¹²³. Він вніс суттєві зміни до правового регулювання діяльності компаній, що надають юридичні послуги за допомогою технологій, особливо в сфері стягнення боргів та масових позовів.

Окрім цього, LegalTech частково охоплюється регулюванням штучного інтелекту. Хоч AI Act (2024) не є актом, що прямо стосується LegalTech, але він регулює системи, що використовують штучний інтелект – зокрема, Legal Bot, системи аналізу рішень або smart-контракти з автономними функціями. І тому, якщо LegalTech-сервіс входить до сфери високого ризику (наприклад, впливає на право на захист, доступ до правосуддя) – він підпадає під обов’язкову реєстрацію, аудит і моніторинг.

Наявні в Німеччині також і судові прецеденти у сфері LegalTech, які з огляду на початок формування відповідного правового поля в Україні варто навести. Так, у 2019 році адвокатська палата Німеччини подала позов проти

¹²² Legal AI startup DoNotPay reaches settlement in customer class action. *Reuters*. URL: <https://www.reuters.com/legal/legalindustry/legal-ai-startup-donotpay-reaches-settlement-customer-class-action-2024-06-06/> (date of access 28.04.2025).

¹²³ Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt : Bundesgesetz vom 10.08.2021 // *Bundesgesetzblatt. Teil I*. 2021. Nr. 53. S. 3415–3419. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*/%5b@attr_id=%27bgbl121s3415.pdf%27%5d <https://www.justsecurity.org/109203/us-ai-action-plan/> (date of access 28.04.2025).

відомої компанії Wolters Kluwer¹²⁴, яка пропонувала онлайн-генератор юридичних документів як платну послугу у сфері LegalTech.

Позивач стверджував, що відповідач надавав юридичні послуги без відповідного дозволу, порушуючи Закон про надання юридичних послуг (RDG) та застосовував оманливі рекламні твердження на противагу Закону про недобросовісну конкуренцію (UWG).

Відповідач заперечував ці твердження, наголошуючи, що його генератор лише автоматизує створення стандартних договорів і не замінює юридичну консультацію.

Федеральний суд Німеччини (BGH) дійшов висновку, що використання автоматизованого генератора для створення стандартних юридичних документів **не є юридичною послугою у розумінні Закону про надання юридичних послуг (RDG)**. Хоча діяльність відповідача включала розробку, надання і створення документів, вона не стосувалася конкретної справи користувача і не передбачала здійснення індивідуальної юридичної оцінки.

У межах розгляду суд підтвердив, що генератор нагадує посібник із формулярами й працює за схемою запитань-відповідей, уникаючи юридичного аналізу конкретних фактів. Водночас Федеральний суд заборонив відповідачу використовувати окремі оманливі формулювання в рекламі.

При цьому було наголошено, що рішення стосується саме запропонованої моделі надання послуг через генератор Smartlaw і не забороняє подальший розвиток LegalTech у сфері стандартних цифрових сервісів, які не передбачають індивідуальної правової підтримки¹²⁵.



Франція. LegalTech у Франції регулюється переважно через загальні суміжні норми права. Окремого спеціалізованого закону, який би комплексно регулював

¹²⁴ Oberlandesgericht Köln. Urteil vom 19.06.2020 – 6 U 263/19. URL: https://nrwe.justiz.nrw.de/olgs/koeln/j2020/6_U_263_19_Urteil_20200619.html (дата звернення: 29 квітня 2025 року).

¹²⁵ Meyer, O., Barreiros, P. L. The German Legal Services Act and the Smartlaw Case: A Precedent for Legal Tech Services in Germany. *Studia Prava Publicznego*. 2025. № 1 (49). С. 31–47. DOI: <https://doi.org/10.14746/spp.2025.1.49.2> (date of access 28.04.2025).

саме LegalTech у Франції наразі немає, однак наявний цікавий кейс, який варто висвітлити.

Починаючи з 2016 року, внаслідок відкриття доступу до судових рішень та розвитку LegalTech-компаній і технологій обробки даних (NLP, машинне навчання) стало можливим масово аналізувати поведінку суддів і прогнозувати їхні рішення на основі відкритих даних. Французькі судді висловили занепокоєння тим, що такі аналітичні інструменти можуть призвести до складання рейтингів суддів, тиску на них, маніпуляцій (наприклад, вибір судді під конкретну справу) та порушення незалежності судової влади.

Велася гостра дискусія між прихильниками повної відкритості судових даних і тими, хто наполягав на захисті ідентичності суддів. Пропонувалося навіть повністю анонімізувати судові рішення, але в результаті було знайдено компроміс: імена суддів залишилися у відкритих рішеннях, однак їх не можна використовувати для статистичного аналізу, оцінки чи прогнозування їхньої професійної діяльності. Тому, у 2019 році було внесено поправки до Закону про відкриті дані (*Loi pour une République numérique*), які забороняють ідентифікувати або оцінювати діяльність окремих суддів на основі відкритих судових рішень за допомогою автоматизованих систем (тобто LegalTech-аналітики). Порушення цієї заборони карається кримінальною відповідальністю – ув'язненням до 5 років та штрафом у розмірі 300 000 євро¹²⁶.



Велика Британія. Окрім загальних нормативно-правових актів, що регулюють відповідну діяльність функціонують в країні також професійно-етичні

ініціативи, ключові з яких варто розкрити. Legal Services Board (LSB) – незалежний орган, який здійснює нагляд за регулюванням юридичних послуг

¹²⁶ France bans judge analytics, 5 years in prison for rule breakers. *Artificial Lawyer*. 2019. URL: <https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/> (date of access 28.04.2025).

в Англії та Уельсі опублікував у 2024 році [нормативні вказівки щодо сприяння технологіям та інноваціям для покращення доступу до юридичних послуг](#)¹²⁷.

LawtechUK – ініціатива, що фінансується Міністерством юстиції Великої Британії та створена у 2019 році для прискорення зростання сектору юридичних технологій Великої Британії. Цілі LawtechUK включають збільшення інновацій та впровадження юридичних технологій у юридичних послугах; покращення розуміння переваг юридичних технологій постачальниками юридичних послуг усіх розмірів; підтримку розвитку технологій для розширення доступу до юридичних послуг та зменшення незадоволених юридичних потреб; підтримку зростання сектору юридичних технологій Великої Британії та його внеску в економіку Великої Британії. Ініціатива реалізується за підтримки організацій CodeBase та Legal Geek. Вона охоплює фінансування проєктів, створення «пісочниць» для тестування технологій (Lawtech Sandbox), запуск навчальних і інноваційних платформ, а також сприяє взаємодії компаній із регуляторами¹²⁸.

The Law Society – професійна організація, яка підтримує своїх членів у впровадженні AI та LegalTech, надаючи поради щодо етичного використання технологій у юридичній практиці. Вона публікує спеціальні звіти, рекомендації та практичні нотатки щодо впровадження LawTech, ризиків, відповідності регуляторним вимогам і захисту даних, допомагає юристам орієнтуватися у нових технологіях, враховувати професійні стандарти у використанні цифрових інструментів в правовій діяльності¹²⁹.

Підсумовуючи: LegalTech — це не просто автоматизація, а новий стиль мислення у праві. Юрист майбутнього має не лише знати норми, а й уміти впроваджувати технології для підвищення доступності, ефективності й прозорості юридичної допомоги. Проте, не дивлячись на те, що LegalTech – це

¹²⁷ Legal Services Board. Statutory guidance on promoting technology and innovation to improve access to legal services: Response to consultation. April 2024. URL: <https://legalservicesboard.org.uk/wp-content/uploads/2024/04/Statutory-guidance-on-promoting-technology-%E2%80%93-response-to-consultation-1.pdf> (date of access 28.04.2025).

¹²⁸ LawtechUK. LawtechUK Ecosystem Tracker Report. April 2024. URL: <https://lawtechuk.io/wp-content/uploads/2024/04/LawtechUK-Ecosystem-Tracker-Report.pdf> (date of access 28.04.2025).

¹²⁹ The Law Society. The Law Society of England and Wales. URL: <https://www.lawsociety.org.uk/> (date of access 28.04.2025).

потужний інструмент, він потребує правового контролю, етичних рамок і людського нагляду. Технологія повинна допомагати праву, а не підміняти його.



ПЕРЕВІРКА ЗНАНЬ

What is true and what is false? Justify your answer.

1. Платформа CaseText (CoCounsel) дозволяє юристу проводити глибинний аналіз позову з використанням штучного інтелекту.
2. У Великій Британії Legal Tech-сервіси повинні отримати окрему ліцензію від ЄС.
3. AxDraft — українська платформа для автоматизованого створення юридичних документів.
4. У Франції заборонено використання аналітики судових рішень для створення рейтингів суддів.
5. В Україні прийнято окремий закон «Про Legal Tech».
6. Право на пояснення автоматизованого рішення регламентується ст. 22 GDPR.
7. Системи smart-контрактів в Україні вже мають повноцінну юридичну силу.
8. Legal Design — це підхід до візуального й зручного представлення правової інформації.
9. Правовий ризик використання систем на базі ШІ у LegalTech полягає в тому, що їхні рішення є прозорими, але надто складними для оскарження.
10. Прогнозування судових рішень є потужним інструментом і може базуватись, у тому числі, на профілюванні суддів.
11. LegalTech і SmartLaw – це ідентичні поняття.

ЗАВДАННЯ

**1. Create Your Own LegalTech Startup**

Створіть та опишіть концепцію нового цифрового продукту для юристів із проведенням аналізу правових ризиків і визначенням шляхів їх мінімізації. Оформіть роботу у форматі презентації або інфографіки.

**2. Analyze the court cases «Upsolve Inc. v. James», «Faridian v. DoNotPay» & «Hamburg Bar Association v. Wolters Kluwer (Smartlaw Case)»**

На підставі проведеного аналізу сформууйте проект нормативно-правових норм, які могли б лягти в основу майбутнього правового регулювання відповідних правовідносин в Україні.

**3. Legal Rebranding**

Створіть стратегію для традиційної юридичної фірми, яка хоче перейти на цифрові сервіси та стати лідером у сфері LegalTech.

**4. Ethical Dilemma: AI vs. Lawyer**

Підготуйте аргументовані роздуми на такі питання:

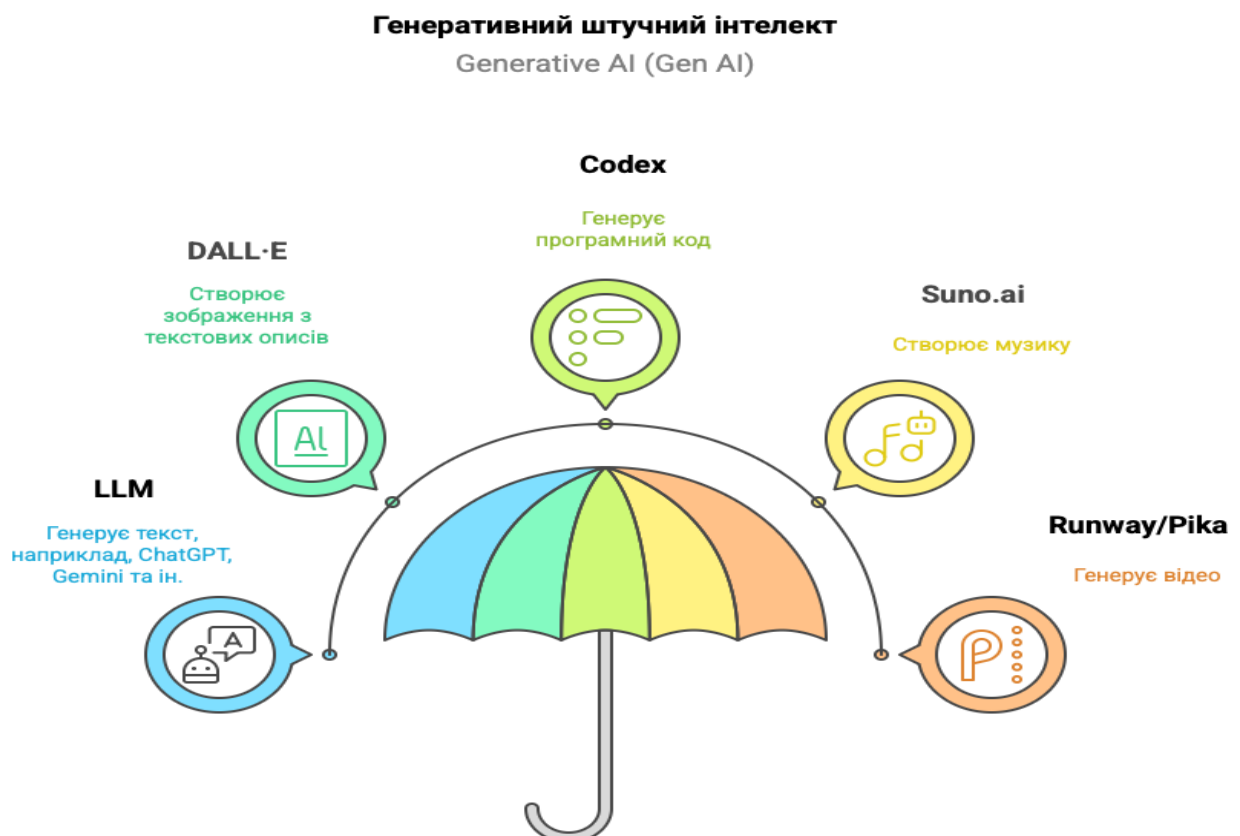
- Чи може штучний інтелект бути суб'єктом відповідальності?
- Чи має існувати юридична відповідальність за помилки, допущені під час надання юридичних послуг із використанням інструментів LegalTech?
- Якщо відповідальність має місце, то хто саме повинен її нести?

Розділ VIII ВЕЛИКІ МОВНІ МОДЕЛІ LARGE LANGUAGE MODELS

1. Базові терміни та принципи роботи

Великі мовні моделі (далі – LLM) відіграють дедалі важливішу роль у професійній діяльності юриста. Із розвитком ШІ значна частина рутинних юридичних завдань може бути виконана за допомогою LLM. У зв'язку з цим особливого значення набуває формування у майбутніх юристів знань про переваги й обмеження використання таких моделей, а також розвиток відповідних цифрових компетентностей. Варто зазначити, що основні ризики, пов'язані із застосуванням LLM, зумовлені технічною природою самих технологій. Відтак для кращого розуміння цих ризиків доцільно насамперед розкрити базові технічні характеристики функціонування LLM.

Досить часто при розкритті інформації про LLM можна зустріти також аббревіатуру GenAI. Щоб краще зрозуміти їх співвідношення нижче подано схему.



Як демонструє схема, GenAI охоплює ширший спектр технологій, серед яких LLM становлять лише один із напрямів. З огляду на характер і специфіку юридичної діяльності, найбільший практичний інтерес становлять саме LLM як інструменти для роботи з текстовою інформацією.

Варто відзначити, що сьогодні існує значне різноманіття моделей LLM. Ключові з них зображено нижче.

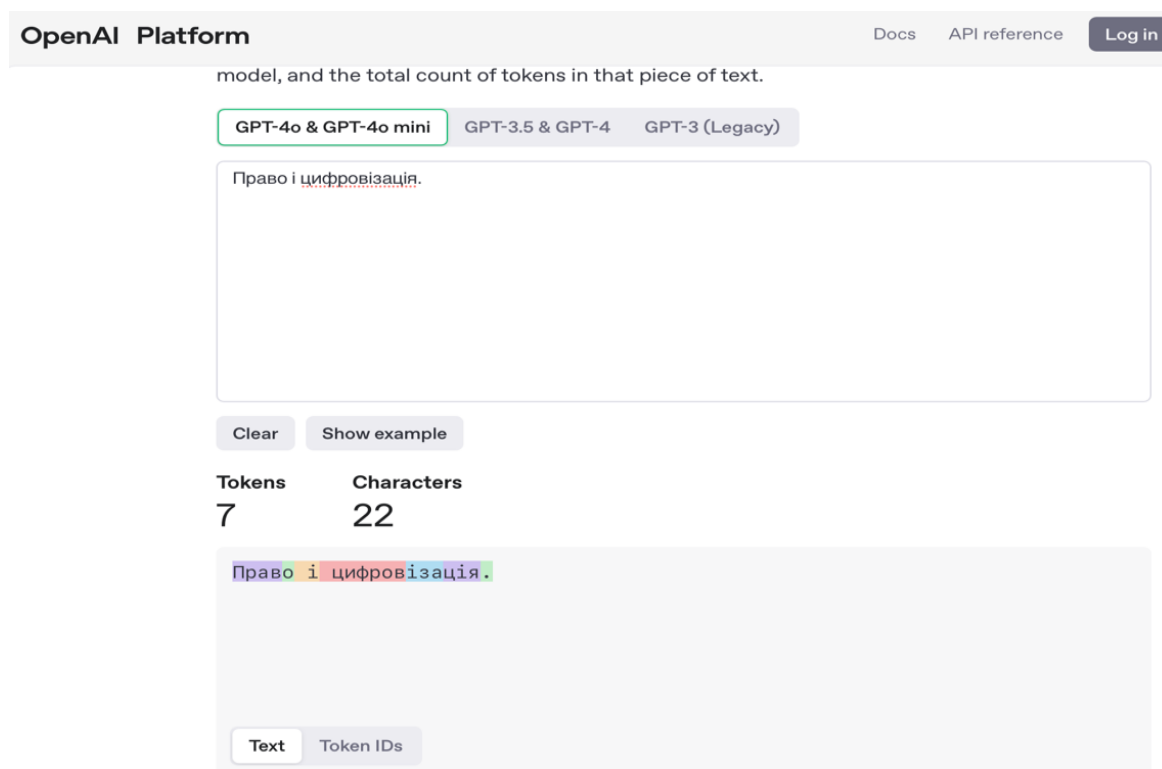


Попри схожість функціонального призначення, моделі LLM відрізняються між собою рядом характерних особливостей, що безпосередньо відображається на результатах роботи з ними. Так, наприклад Perplexity, згідно з окремими спостереженнями, продемонструвала кращі результати під час проходження тестів з українського права (порівняно з такими моделями як ChatGPT, Claude, Gemini, Copilot), що автори пояснюють доступом цієї моделі до інтернету та використанням релевантних джерел. Водночас, дана модель іноді формує некоректну аргументацію, навіть якщо сама відповідь є правильною [с. 186]¹³⁰. Також, наприклад, існує твердження, що моделі LLM розроблені у Китаї, часто демонструють орієнтацію на китайський контент, оскільки вони навчалися переважно на китайських джерелах даних. Тому користувач повинен самостійно

¹³⁰ Юридичні інновації та стартапи / за заг. ред. В.Ю.Пряміцина. Київ, 2024. 290 с.

методом спроб визначити для себе оптимальну модель LLM для використання, враховуючи технічні характеристики, доступність (фінансову, мовну) та якість результату. Власне, на чому ґрунтується результат роботи LLM – допоможе зрозуміти базове технічне розуміння процесів роботи LLM.

Отже, насамперед слід зазначити, що LLM, отримуючи вхідний запит у текстовому форматі, не обробляє його безпосередньо як суцільний текст. Спочатку введене повідомлення передається до токенизатора — спеціального компонента, який перетворює текст на послідовність токенів, тобто елементарних одиниць інформації, що можуть бути окремими словами, частинами слів або навіть окремими символами. Ілюстрація відображає принцип роботи токенизатора, який можна самостійно перевірити у дії за допомогою [інтерактивного симулятора](https://platform.openai.com/tokenizer)¹³¹.



Кожному токенові відповідає певний числовий індекс. На основі цього індексу за допомогою спеціальної матриці формується його векторне (кодоване) представлення, яке і подається до моделі LLM. Остання, аналізуючи контекст

¹³¹ Tokenizer. *OpenAI*. URL: <https://platform.openai.com/tokenizer> (date of access: 07.04.2025).

попередніх tokenів, формує ймовірнісний прогноз наступного токена. Важливо підкреслити, що модель на кожному кроці здатна передбачити лише один токен, після чого процес повторюється: новий токен додається до вхідної послідовності, і на його основі передбачається наступний (такий покроковий цикл отримання наступного токена називають ітерацією)¹³².

За бажанням, можна ознайомитися докладніше з:

- цікавими фактами щодо функціонування LLM¹³³



- інтерактивною візуалізацією процесу tokenізації та типами



tokenізаторів^{134, 135}.



Передбачення наступного токена ґрунтується на ймовірностях: модель «оцінює», який токен найімовірніший у даній позиції. Відповідний процес представлено у схемі¹³⁶ нижче.

Запит	Tokenізація	LLM	Ймовірність	Результат
Конституція України гарантує...			“права” 0.41 “свободи” 0.22 “право” 0.15 “освіту” 0.05 “автономію” 0.01 ... (тисячі інших) ...	права

Модель обчислює ймовірності для кожного наступного токена залежно від температури генерації. **Температура LLM** – це параметр, який керує

¹³² Castelluccio C. Introduction to Generative AI and Large Language Models. URL: <https://github.com/microsoft/generative-ai-for-beginners/tree/main/01-introduction-to-genai#how-do-large-language-models-work> (date of access: 07.04.2025).

¹³³ Large Language Models explained briefly. URL: <https://www.youtube.com/watch?v=LPZh9BOjkQs> (date of access: 07.04.2025).

¹³⁴ LLM Tokenizers Explained: BPE Encoding, WordPiece and SentencePiece. URL: <https://www.youtube.com/watch?v=hL4ZnAWSyuU> (date of access: 07.04.2025).

¹³⁵ Mastering Tokenization in NLP: The Ultimate Guide to Unigram and Beyond! URL: <https://www.youtube.com/watch?v=RAIUJ3VFXmI> (date of access: 07.04.2025).

¹³⁶ Схему розроблено на основі навчального відео: LLM Foundations: Understanding Tokenization & Training: Chapter 4. URL: <https://www.youtube.com/watch?v=LZ2gr04q7Hk&t=104s> (date of access: 07.04.2025).

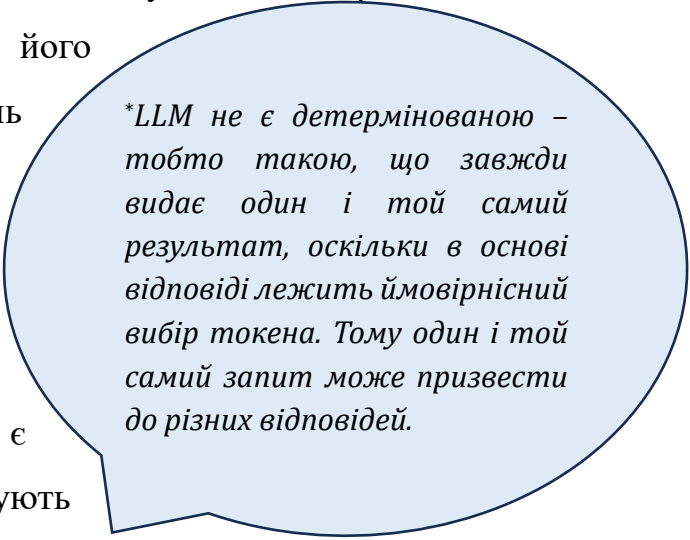
випадковістю або креативністю відповідей моделі. Так, відповідна температура, як правило, коливається від 0.0 до 1.0 (технічно можливі значення й до 2.0).

➤ При високій температурі (наприклад, від 0,7-1.0) – модель вибирає токен випадково у передбачених ймовірностях (тобто, як показано в прикладі, може вибрати «свободи» навіть якщо «права» має більшість шансів). Висока температура дозволяє моделі використовувати більше варіативності та фантазії, може вигадати щось нове, несподіване.

➤ При низькій температурі (наприклад, від 0.01-0.3) – модель майже завжди вибирає найімовірніший токен (як в прикладі – «права»). Модель, в такому випадку, діє «обережно», видає передбачувані, точні, формальні відповіді.

Таким чином, LLM здатна обирати або найбільш ймовірніший токен, або один із менш ймовірних – залежно від встановлення температури. Це дозволяє бути моделі гнучкою: іноді – точною, іноді – творчою. Водночас, як засвідчує технічний аналіз принципів функціонування моделі, навіть за низьких значень температури (наприклад, 0,1) можлива генерація креативного контенту, що потенційно впливає на достовірність сформованих відповідей.

Тому, як було слушно зазначено: «Результати генеративного ШІ не є бездоганними: у деяких випадках його «творчість» призводить до викривлень реальності або образливих висловлювань. Такі моделі не мають інтелекту в повному значенні цього терміна, зокрема критичного чи емоційного мислення. Вони не є детермінованими* й не гарантують достовірності, оскільки можуть переконливо поєднувати правдиву інформацію з вигаданою»¹³⁷.



**LLM не є детермінованою – тобто такою, що завжди видає один і той самий результат, оскільки в основі відповіді лежить ймовірнісний вибір токена. Тому один і той самий запит може призвести до різних відповідей.*

З вище сказаного можна зробити важливий висновок:

¹³⁷ Castelluccio C. Introduction to Generative AI and Large Language Models. URL: <https://github.com/microsoft/generative-ai-for-beginners/tree/main/01-introduction-to-genai#how-do-large-language-models-work> (date of access: 07.04.2025).

- температуру 0.1-0.3 – варто використовувати для юридичних, технічних, фактологічних текстів, коли потрібна точність і надійність;
- температуру 0.4-0.7 – краще використовувати для діалогів, творчих завдань;
- температуру 0.8-1.0 і вище – для генерації ідей, поезії, художніх текстів, креативу.

Варто зазначити, температура налаштовується по-різному залежно від моделі: при роботі через API її задають вручну (наприклад, у юридичних стартапах). Натомість у готових застосунках, зокрема в ChatGPT, параметр встановлений за замовчуванням і, як правило, не змінюється користувачем безпосередньо. Вважається, що GPT-3.5 працює з температурою приблизно 0.7, тоді як GPT-4-turbo використовує динамічний діапазон температур, орієнтовно в межах 0.2–1.0, залежно від типу запиту.

Ефективність взаємодії з LLM залежить від якісних запитів, що є сферою **prompt-інженерії** – практики створення оптимальних вхідних даних, яка також дозволяє умовно регулювати температуру моделі. Наприклад, формулювання на кшталт *«Відповідай максимально чітко, офіційно, без відхилень»* спонукає модель діяти так, ніби температура дорівнює 0.2. Натомість запити типу *«Додай більше креативу, прикладів»* активізують поведінку, характерну для вищих температур (приблизно 0.8–1.0).

Іншими способами підвищення ефективності відповідей моделей є використання так званих метапідказок (**metaprompting**) та заземлення (**grounding**)¹³⁸. Метापідказка – це інструкція, яка визначає роль та стиль моделі під час генерування відповіді, наприклад, *«Ти – професійний юрист, який спеціалізується на праві ЄС. Твоє завдання – відповідати коротко, точно, посилаючись лише на офіційні джерела»*. Заземлення передбачає обмеження джерел, на які може спиратися модель, конкретними, перевіреними даними – наприклад, нормативно правовими актами, судовими рішеннями, підручниками

¹³⁸ Prompt Engineering Fundamentals. URL: https://github.com/microsoft/generative-ai-for-beginners/blob/main/04-prompt-engineering-fundamentals/README.md?WT.mc_id=academic-105485-koreyst (date of access: 07.04.2025).

тощо. Приклад заземлення: «*Ось уривок із статті Конституції України На основі цього поясни*». Зазначені методи суттєво підвищують якість, точність і достовірність відповідей, зменшуючи ризик вигаданих або неточних тверджень (так званих галюцинацій).

Ознайомитися з прикладами ефективних промтів у сфері освіти можна, перейшовши до GitHub-репозиторію Microsoft – [Prompts for Educators](#)¹³⁹. Також нижче надані інші корисні посилання:

- [для чого потрібні і як налаштувати ChatGPT Custom instructions](#)¹⁴⁰;
- [як налаштувати LLM в ролі персоналізованого репетитора англійської мови](#)¹⁴¹;
- [практичні поради для науковців з використання LLM](#)¹⁴²;
- [рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти](#)¹⁴³.

Окрім цього автором розроблено посібник для студентів та викладачів «LLMs in Ukrainian Higher Education: A Practical Guide for Students and Lecturers. Великі мовні моделі в українській вищій освіті: практичний посібник для студентів та викладачів»¹⁴⁴. Він може слугувати зразком для інших університетів в Україні з метою регулювання відповідної політики освітнього процесу з врахуванням цифрових викликів сьогодення.

¹³⁹ Prompts for Education: Enhancing Productivity & Learning. URL: <https://github.com/microsoft/prompts-for-edu?tab=readme-ov-file> (date of access: 07.04.2025).

¹⁴⁰ ChatGPT Custom instructions. Власні інструкції для ChatGPT перед запитом. Персоналізація ChatGPT. Learn to Earn Global. URL: <https://www.youtube.com/watch?v=C51cNtK8KT8> (дата звернення: 07.04.2025).

¹⁴¹ Ушаков В. Вивчай Англійську БЕЗКОШТОВНО з ChatGPT. URL: <https://www.youtube.com/watch?v=REpWq3uNSAM> (дата звернення: 07.04.2025).

¹⁴² Промпти для Вчених у ChatGPT: Як Використовувати ІІІ для Наукових Досліджень? *Наукові публікації*. URL: <https://www.youtube.com/watch?v=inCEGs2mzuA> (дата звернення: 07.04.2025).

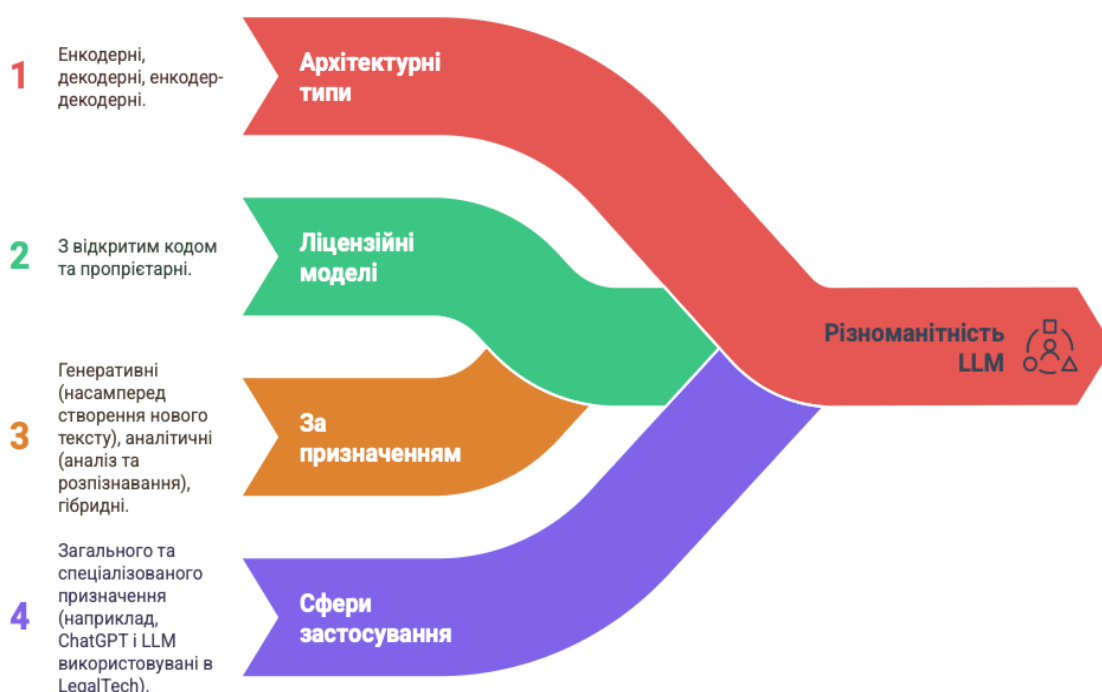
¹⁴³ Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти. Квітень 2025. URL: <https://mon.gov.ua/static-objects/mon/sites/1/news/2025/04/24/shi-v-zakladakh-vyshchoi-osvity-24-04-2025.pdf> (дата звернення: 07.05.2025).

¹⁴⁴ Костенко Світлана. LLMs in Ukrainian Higher Education: A Practical Guide for Students and Lecturers. Великі мовні моделі в українській вищій освіті: практичний посібник для студентів та викладачів. Житомир: Поліський національний університет, 2025. 21 с.

2. Класифікації LLM

LLM можуть суттєво відрізнятися між собою залежно від архітектури, навчальних даних і сфери застосування. Усвідомлення цих відмінностей є важливим, зокрема для вибору відповідної моделі у сфері юридичних технологій або під час запуску правового стартапу.

Узагальнена класифікація LLM



Дві останні згадані групи LLM є інтуїтивно зрозумілими та не вимагають розгорнутого тлумачення. Натомість перші дві передбачають використання спеціалізованої термінології, що зумовлює необхідність їхнього короткого пояснення. У зв'язку з цим доцільно подати їхню стислу характеристику.

Одним із базових критеріїв класифікації є рівень відкритості доступу до моделі: розрізняють моделі з відкритим кодом (open-source) та пропріетарні моделі (proprietary).

Моделі з відкритим програмним кодом – це такі LLM, архітектура та вихідний код яких є загальнодоступними. Вони зазвичай розробляються дослідницькими центрами, університетами або технологічними компаніями з

метою забезпечення прозорості та гнучкості використання. Користувачі можуть вільно переглядати, модифікувати та адаптувати такі моделі до власних потреб. Однак ці моделі не завжди оптимізовані для промислового використання, можуть поступатися за продуктивністю комерційним аналогам, а також часто обмежені в технічній підтримці, оновленнях та доступі до ресурсів. Прикладами таких моделей є Alpaca, BLOOM, LLaMA.

Пропрієтарні моделі – це LLM, які перебувають у власності приватних компаній і не передбачають відкритого доступу до коду або можливості його змінення. Вони, як правило, спеціально адаптовані для масштабного застосування у виробничому середовищі, характеризуються високою стабільністю, безперервною підтримкою та регулярними оновленнями. Використання таких моделей здійснюється на основі ліцензійних угод, передплат або інших комерційних умов. Користувачі, як правило, не мають доступу до даних, на яких модель навчалась, що вимагає довіри до політики конфіденційності та етичних стандартів компанії-розробника. Відомі приклади – GPT (OpenAI), Gemini (Google), Claude (Anthropic)¹⁴⁵.

Підсумовуючи, LLM з відкритим кодом – це моделі, які можна вільно використовувати, змінювати та запускати у власному середовищі, тоді як пропрієтарні моделі – це закриті рішення, що використовуються відповідно до умов компанії-правовласника.

Нижче подано порівняльну таблицю відкритих і пропрієтарних LLM.

Критерій	LLM відкритого коду (Open-source)	Пропрієтарні LLM (Proprietary)
Приклади	Mistral, LLaMA (Meta), Falcon, GPT-J, BLOOM	GPT-4 (OpenAI), Claude (Anthropic), Gemini (Google)
Доступ до коду	✓ Відкритий код і архітектура (на GitHub та ін.)	✗ Код і дані закриті

¹⁴⁵ Castelluccio C., Lopes P. Exploring and comparing different LLMs. URL: https://github.com/microsoft/generative-ai-for-beginners/blob/main/02-exploring-and-comparing-different-llms/README.md?WT.mc_id=academic-105485-koreyst (date of access: 07.04.2025).

Критерій	LLM відкритого коду (Open-source)	Пропрієтарні LLM (Proprietary)
Спосіб використання	Можна запускати локально, без інтернету	Доступ тільки через API або платформи (наприклад, ChatGPT)
Модифікація/адаптація	✓ Дозволено адаптувати під власні цілі (напр. для права)	✗ Заборонено змінювати або запускати самостійно
Вартість	Переважно безкоштовні, але потребують дорогих серверних та обчислювальних ресурсів	Зазвичай платні, залежно від провайдера
Підтримка	Спільнота (як Wikipedia або Linux), неофіційна	✓ Офіційна техпідтримка, документація
Прозорість	✓ Повна прозорість, можна дослідити «як працює модель»	✗ Обмежений або відсутній доступ до внутрішньої логіки
Контроль над даними	✓ Дані залишаються на локальному сервері	✗ Можлива обробка/збереження даних провайдером
Кастомізація	✓ Повна свобода змін	✗ Неможлива або дуже обмежена
Якість генерації	Добра, але часто поступається топовим пропрієтарним моделям	✓ Висока якість (особливо GPT-4, Claude 3)
Технічні вимоги	¶ Потрібні знання для запуску/налаштування	✓ Все вже налаштовано
Юридична/наукова придатність	✓ Підходять для обробки конфіденційних або специфічних юридичних даних	✗ Ризик витоку або сторонньої обробки

З урахуванням специфіки моделей з відкритим кодом та пропрієтарних рішень, доцільно зробити такий висновок: **у випадках, коли необхідно забезпечити локальну інтеграцію, контроль над даними та конфіденційність** (наприклад, при створенні систем ШІ для аналізу рішень Конституційного Суду України або національного законодавства),

оптимальним вибором є LLM з відкритим кодом. Вони дозволяють адаптацію моделі до конкретного правового контексту та її розгортання у захищеному середовищі.

Натомість для завдань, що вимагають високого рівня генеративної якості, узагальнення інформації чи ведення складного діалогу (зокрема, створення чат-бота репетитора з певної галузі права), **ефективнішими є пропрієтарні моделі**, які демонструють вищу стабільність, креативність і мовну природність.

Ще одним важливим критерієм класифікації LLM є тип їхньої архітектури. Це визначає, як саме модель обробляє, аналізує й генерує текстову інформацію, тобто, яким чином вона «мислить» під час виконання завдань. Залежно від цього, мовні моделі поділяють на **енкодерні, декодерні та універсальні (енкодер-декодерні)**. Кожен із цих типів має свої переваги й обмеження, що впливають на доцільність їх застосування у певних правових, дослідницьких чи бізнес-контекстах.

Енкодерні моделі (encoder-only). Цей тип моделей спеціалізується на розумінні тексту, тобто аналізі, класифікації, пошуку смислових залежностей, виявленні фактів тощо. Вони створені для того, щоб «читати» інформацію та представляти її у вигляді векторних структур. Це робить їх надзвичайно ефективними для завдань, що не потребують генерації тексту, зокрема для пошукових систем, юридичної аналітики, виявлення правових норм або класифікації судових рішень.

Одним із найвідоміших прикладів є модель BERT (Bidirectional Encoder Representations from Transformers), яка широко використовується в системах інформаційного пошуку та юридичному документуванні.

Декодерні моделі (decoder-only). Ці моделі, навпаки, фокусуються на генерації тексту. Вони використовуються для створення відповідей у чат-ботах, написання резюме, автоматизованого складання правових документів або пояснення складних норм у доступній формі. Декодерна архітектура забезпечує послідовне передбачення наступного слова на основі попередніх, що робить її

придатною для завдань, пов'язаних із креативним або логічно узгодженим письмом.

До цієї категорії належать найбільш відомі моделі, зокрема GPT (Generative Pre-trained Transformer), які вже успішно застосовуються в освітніх юридичних платформах, інтелектуальних помічниках юриста чи в системах автоматизованого складання договорів.

Універсальні моделі (encoder-decoder або sequence-to-sequence). Це комбіновані моделі, що поєднують можливості аналізу тексту (енкодер) та його генерації (декодер). Вони є особливо ефективними в ситуаціях, коли потрібно не лише зрозуміти запит, а й сформулювати обґрунтовану відповідь – наприклад, під час автоматизованого перекладу юридичних документів, перефразування нормативних положень або відповіді на складні запити в правничому чат-боті.

Типовим прикладом є T5 (Text-to-Text Transfer Transformer) та BART, що активно використовуються в багатомовних юридичних системах або в системах підтримки прийняття рішень, де важлива якість як аналізу, так і формулювання.

Порівняльна характеристика архітектур LLM:

Тип архітектури	Основне призначення	Переваги
Енкодерні	Аналіз і розуміння тексту	Точність класифікації, пошуку, розпізнавання сутностей
Декодерні	Генерація тексту	Плавність, зв'язність і логіка відповіді
Енкодер-декодерні	Повний цикл: аналіз + генерація	Баланс розуміння та генерації, універсальність

Отже, вибір між енкодерною, декодерною чи універсальною архітектурою LLM має ґрунтуватися на характері завдань, які стоять перед користувачем. У випадках, коли необхідно проаналізувати великі обсяги правових текстів, класифікувати норми чи виявити юридичні патерни, найефективнішими є енкодерні моделі. Для генеративних завдань – створення шаблонів документів, відповідей у правничому чат-боті, пояснень складного юридичного тексту – доцільно обирати декодерні моделі. А у випадках, коли важливо забезпечити як глибоке розуміння тексту, так і його формулювання (наприклад, при побудові

системи юридичного перекладу або відповіді на змістовні запити), найкраще себе проявляють універсальні моделі.

3. Навички роботи з LLM як професійна необхідність юриста

У сучасній юридичній практиці володіння навичками ефективної роботи з LLM поступово стає не просто перевагою, а необхідністю. Для тих правників, які вже оцінили як потенціал, так і загрози, пов'язані з цими технологіями, LLM стали незамінними інструментами у повсякденній роботі. З поширенням знань про ці моделі, їх популярність серед користувачів лише зростає. Більше того, цифрові компетентності у сфері LLM дедалі частіше розглядаються як чинник конкурентної переваги на ринку праці.

Водночас юридична сфера вимагає особливої обережності при застосуванні LLM, оскільки будь-яка помилка може мати серйозні наслідки як для окремого юриста, так і для системи правосуддя загалом. Відсутність розуміння принципів роботи таких моделей або надмірна довіра до їх відповідей уже призвели до низки резонансних інцидентів.

Так, у США, адвокати з Нью-Йорка, використавши вигадані ChatGPT судові прецеденти, були оштрафовані на \$5 000. Інші приклади – надання фальшивих правових посилань у справах Майкла Коена, використання ChatGPT для обґрунтування судових витрат на суму понад \$113 000 (які суд визнав необґрунтованими), або включення в документи посилань на справи, яких не існує¹⁴⁶. В усіх випадках суди вказували на неприпустимість покладання на генеративні моделі без ретельної перевірки.

Схожі приклади мають місце й в Україні. У 2024–2025 роках в українських судах неодноразово фіксувалися випадки, коли сторони намагалися використовувати відповіді ChatGPT або інші генеративні матеріали як докази чи тлумачення права. Верховний Суд розцінив подібні дії як прояв зневаги до

¹⁴⁶ Nicola Fabiano. AI Act and Large Language Models (LLMs): When critical issues and privacy impact require human and ethical oversight. *International Institute of Informatics and Systemics (IIIS)*. USA. May 2, 2024. URL: <https://arxiv.org/html/2404.00600v1> (date of access: 23.04.2025).

судової влади, а інші суди прямо вказували на неприйнятність використання результатів ШІ як заміни експертних висновків чи доказів¹⁴⁷.

Судова практика чітко показує, що неволодіння принципами роботи з LLM та відсутність цифрової грамотності у цій сфері можуть дискредитувати юриста та підірвати довіру до судової системи. Навпаки, обізнаність щодо функціонування LLM, їхніх сильних і слабких сторін, є запорукою відповідального та ефективного застосування таких інструментів.

Власне тому, задля запобігання подібним помилкам необхідно інтегрувати цифрову підготовку, зокрема й роботу з LLM, у структуру юридичної освіти. Йдеться не лише про загальні уявлення про штучний інтелект, а про цілеспрямоване навчання методам перевірки фактів, виявлення штучних «галюцинацій», оцінки достовірності та правової релевантності згенерованих відповідей.

Розвиток цифрових технологій у сфері права (LegalTech, електронні суди, автоматизовані інструменти доказування тощо) ставить перед юристами нові виклики. Вони більше не можуть бути лише фахівцями з права – їм необхідно стати й впевненими користувачами цифрових рішень, які здатні критично аналізувати інформацію, створену за допомогою ШІ. Таким чином, навички роботи з LLM – це вже не просто технічний інструмент, а складова професійної етики, юридичної відповідальності та академічної доброчесності.



ПЕРЕВІРКА ЗНАНЬ

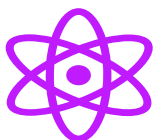
What is true and what is false?

Justify your answer.

¹⁴⁷ Костенко С.О. Помилки, що коштують репутації: навіщо юристу розуміти роботу з LLM. Забезпечення правопорядку в умовах воєнного стану та мировідбудови : зб. наук. ст. за матеріалами ІІІ Всеукр. наук. - практ. конф. (Житомир, 1 травня 2025 р.) Житомир: Поліський національний університет, 2025. С. 31-34.

1. Модель GPT-4 є відкритою (open-source) і кожен охочий може переглянути її архітектуру та навчальні дані.
2. Енкодерні моделі зазвичай не використовуються для створення чат-ботів.
3. LLM можуть помилятися або вигадувати факти, навіть якщо вони звучать переконливо.
4. Пропріетарні моделі завжди кращі за моделі з відкритим кодом.
5. LLM здатні працювати офлайн на локальному сервері без підключення до інтернету.
6. Тип архітектури LLM (енкодер, декодер, енкодер-декодер) безпосередньо впливає на її функціональне призначення.
7. LLM не можна використовувати в правовій сфері через ризик конфіденційності.
8. Для ефективного використання LLM у науковій діяльності не потрібно розуміти принципи її роботи.
9. Великі мовні моделі можуть бути донавчені на спеціалізованих юридичних текстах.
10. LLM завжди дають однаково точні результати незалежно від мови запиту.
11. Використання LLM у дослідженнях потребує критичного мислення та перевірки джерел.

ЗАВДАННЯ



1. Ethical dilemma: automatic contract drafting

Ви – юрист у юридичній фірмі, яка планує впровадити LLM для генерації проектів договорів оренди. Керівництво запевняє, що модель зекономить час і гроші. Але вам стало відомо, що LLM була навчена на загальних текстах, а не на спеціалізованому праві вашої країни.

Questions:

Чи є етичним використання такої моделі без донавчання на національному праві? Які ризики для клієнтів і фірми можуть виникнути? Обґрунтуйте свою позицію.

**2. Court decision vs LLM: whom to trust?**

У межах дослідження студент запитав у LLM правовий аналіз ситуації щодо звільнення працівника. Відповідь моделі суперечила висновку Верховного Суду у справі з подібними обставинами.

Questions:

Чи можна вважати відповідь LLM авторитетним джерелом для юридичних висновків? Знайдіть відповідь на це питання у судовому рішенні України. Як студенту перевірити достовірність інформації отриманої від LLM?

**3. Data confidentiality: risks of using LLMs in the public sector**

Уявіть, що Міністерство юстиції планує використовувати LLM для аналізу текстів кримінальних справ. Модель є пропрієтарною, працює на зовнішньому сервері, а дані справ не були анонімізовані.

Questions:

Які правові ризики виникають при такому підході? Чи є порушення вимог конфіденційності? Як можна вирішити цю проблему з урахуванням міжнародного досвіду?

**4. LLM in judicial proceedings: aid or threat?**

22.2.2024 р. юридична фірма Cuddy попросила місто Нью-Йорк сплатити свої судові витрати (понад 113 000 доларів США плюс відсотки), кількісно визначені ChatGPT в успішно врегульованій судовій справі. Однак, Окружний суддя США Пол Енгельмайер присудив трохи більше 53 000 доларів і розкритикував фірму за використання інструменту штучного інтелекту,

«оскільки підтримка його агресивної плати абсолютно і надзвичайно непереконлива»¹⁴⁸.

Questions:

Чи є використання LLM у судовому процесі допустимим? Де проходить межа між інструментом допомоги і делегуванням професійної відповідальності?

**5. Regulating LLMs in law: necessity or overregulation?**

Деякі країни запроваджують нормативні акти щодо використання LLM, зокрема для запобігання дискримінаційним або неточним відповідям. Інші вважають, що це стримує інновації.

Questions:

Яка ваша позиція щодо державного регулювання великих мовних моделей у правовій сфері? Як досягти балансу між свободою технологій і правовою відповідальністю?

¹⁴⁸ Fabiano N. AI Act and Large Language Models (LLMs): When critical issues and privacy impact require human and ethical oversight. URL: <https://arxiv.org/html/2404.00600v1#bib.bib24> (date of access: 07.04.2025).

Розділ IX ПРАВОВИЙ ДИЗАЙН

LEGAL DESIGN

1. Поняття та історія

Правовий дизайн (legal design) – це міждисциплінарний підхід, що поєднує право, дизайн-мислення та технології для створення більш зрозумілих, доступних і ефективних юридичних процесів та документів. Цей напрямок набуває популярності в усьому світі, включаючи Україну, і стає важливим інструментом для модернізації правової системи.

Історичні передумови



➤ 1. Передумови виникнення (до 1990-х років)

Ще з давніх часів юристи намагалися зробити правові тексти більш зрозумілими: кодифікація законів у Стародавньому Римі (зокрема, Corpus Juris Civilis Юстиніана) мала на меті упорядкувати і спростити право для суддів і громадян.

У XIX–XX століттях почали з'являтися спроби спростити юридичні документи, особливо в англо-американській системі права (наприклад, рух за «Plain Language in Law» – за просту мову в праві). Однак це були лише окремі ініціативи, не системний підхід.

➤ 2. Початок візуалізації права (1990-ті роки)

В цей час активно створюються роботи на тему «правової візуалізації» (Legal Visualization), що заклали інтелектуальну основу для подальшого розвитку юридичного дизайну. Крім того, розвиваються графічні технології, UX-дизайн, що також вплинуло на підхід до уявлення інформації в різних сферах, в тому числі і у праві.

➤ 3. Формування концепції юридичного дизайну (2000–2010 роки)

Із розвитком дизайн-мислення (Design Thinking) у Стенфордському університеті виникла ідея застосувати цей підхід до сфери права.

Юристи починають активно говорити про потребу:

- спростити мову юридичних текстів;
- зробити договори більш «людиноорієнтованими» (user-friendly);
- візуалізувати правові процеси для кращого доступу до правосуддя.

➤ 4. Інституціоналізація юридичного дизайну (після 2013 року)

2013 рік – створення Legal Design Lab у Стенфордському університеті (США) під керівництвом Маргарет Хаган (Margaret Hagan).

Ця лабораторія вперше почала розробляти юридичні проєкти, керуючись методами дизайн-мислення.

Поява першого Legal Design Summit у Гельсінкі (2017), який об'єднав юристів, дизайнерів, розробників і представників судової влади з усього світу.

➤ 5. Сучасний етап розвитку (2017–2025)

Юридичний дизайн активно застосовується у:

- розробці зрозумілих договорів (clear contracts);
- спрощенні користувацьких інтерфейсів для юридичних сервісів;
- створенні інтерактивних форм правової допомоги (онлайн-калькулятори, візуальні гіди).

Поняття «contract design» (дизайн договору) стало окремим напрямом, що фокусується на створенні візуально структурованих і зручних договорів. Багато великих компаній (наприклад, Airbus, IBM, Deloitte) запроваджують принципи юридичного дизайну в щоденну роботу. Розвиток штучного інтелекту, автоматизація юридичних послуг і «право як послуга» (Law as a Service) ще більше підсилюють значення юридичного дизайну¹⁴⁹.

Що ж таке правовий дизайн?

Правовий дизайн – це застосування принципів дизайн-мислення до правової сфери з метою зробити юридичні системи та послуги більш орієнтованими на людину, зручними та задовольняючими потреби користувачів. Це означає переосмислення юридичних процесів і документів,

¹⁴⁹ Юридичні інновації та стартапи: підручник для правників; колектив авторів: за загальною редакцією В. Ю. Пряміцина. Київ, 2024. 290 с.

щоб вони були зрозумілішими та доступнішими для звичайних людей, а не лише для юристів.

2. Принципи правового дизайну

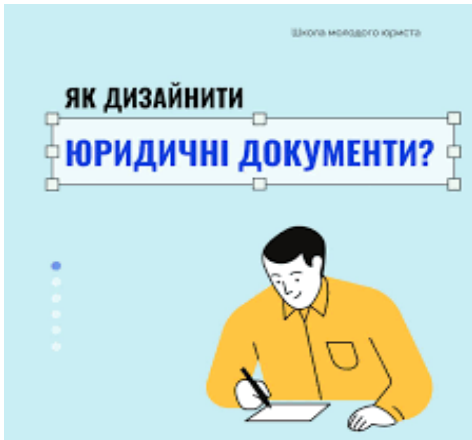


Принципи правового дизайну відображають нове бачення взаємодії людини з правом. Вони зосереджені на тому, щоб зробити право більш зрозумілим, доступним і зручним для користувачів.

Основою юридичного дизайну є переконання, що ефективна юридична система повинна не лише формально відповідати вимогам закону, а й реально допомагати людям орієнтуватися в їхніх правах і обов'язках. Таким чином, юридичний дизайн перетворює право на сферу, де головним є не тільки дотримання норм, але й комфорт та зрозумілість для людини.

Принцип юридичного дизайну	Коротке пояснення	Приклад застосування
Орієнтація на користувача	Створення юридичних продуктів, зручних для кінцевого споживача	Договір оренди житла написаний простою мовою без складних юридичних термінів
Візуалізація	Використання схем, інфографіки та піктограм для пояснення правових норм	Графічна схема етапів судового процесу, яку отримує клієнт при подачі позову
Прототипування і тестування	Створення і перевірка пробних версій юридичних документів чи сервісів	Тестова версія мобільного додатку для реєстрації шлюбу через державний портал
Інтердисциплінарність	Співпраця юристів, дизайнерів, програмістів та інших спеціалістів	Спільна розробка юридичної платформи для електронних заповітів
Прозорість і простота	Використання чіткої структури, простої мови, коротких речень	Замість «укладання правочину про відступлення зобов'язань» пишуть «передача боргу»

3. Етапи процесу правового дизайну



Юридичний дизайн – це не просто оформлення текстів у приємному стилі. Це цілий процес переосмислення права, що базується на дослідженні користувачів, творчості, експериментах і постійному вдосконаленні.

Практична робота у сфері юридичного дизайну проходить у декілька етапів:

1. Дослідження користувачів (User Research)

На початковому етапі здійснюється глибоке дослідження цільової аудиторії та існуючого юридичного контенту. Важливо зрозуміти, хто користується документами чи послугами, якими є їхні потреби, очікування і труднощі. Аналіз включає також виявлення проблемних моментів у текстах: складна термінологія, перевантаженість інформацією, неінтуїтивна структура тощо.

Метою є зрозуміти справжні потреби людей, які будуть користуватися юридичним продуктом. Для цього визначають, хто буде основними користувачами (наприклад, клієнти банку, пацієнти клініки, покупці товару). Проводять глибинні інтерв'ювання, опитування, аналізують поведінку користувачів. Виявляють проблемні точки: які місця у документах незрозумілі, які процеси викликають розгубленість або страх.

Приклад: в опитуванні клієнтів страхових компаній з'ясували, що 60% людей не можуть зрозуміти, в яких випадках їм відмовлять у виплаті.

2. Визначення проблеми (Problem Framing)

Після збору даних формуються конкретні цілі для проекту юридичного дизайну. Це може бути спрощення юридичних текстів, розробка візуальної навігації по документу, покращення інтерфейсу юридичної послуги або оптимізація процесу взаємодії користувачів із системою.

Основною ціллю є правильно сформулювати завдання перед командою. Для цього формують проблему через фокус на користувача: «Як допомогти

людині швидко зрозуміти свої права у разі страхового випадку?» Виділяють пріоритетні сфери для змін.

Приклад: проблема – занадто довгі і незрозумілі умови договору страхування.

3. Генерація ідей (Ideation)



Основна мета цього етапу – створити якомога більше варіантів вирішення задачі без обмежень на початковій стадії. Ідеація заохочує мислення поза межами стандартних юридичних практик та сприяє появі інноваційних підходів. У процесі можуть використовуватися такі методи, як брейнштормінг, ментальні карти (mind

mapping), скетчинг і сценарне моделювання. Важливо забезпечити відкриту атмосферу, де кожна ідея приймається без критики. Після первинної генерації починається етап аналізу й обговорення ідей: оцінюються їхня реалістичність, юридична коректність, користувацька зручність та відповідність цілям проєкту. Відібрані ідеї стають основою для створення перших прототипів документів або процесів, які пізніше тестуються й удосконалюються.

Приклад ідей: створити візуальні дорожні карти для роз'яснення процесу страхових виплат. Додати на сайт калькулятор для розрахунку виплати.



4. Створення прототипів (Prototyping)

Створення прототипів є ключовим етапом у процесі юридичного дизайну, на якому ідеї набувають конкретної форми. Прототип – це попередня версія продукту або документа, створена для тестування і вдосконалення. Прототипи дозволяють швидко і наочно побачити, як виглядатиме

кінцевий результат, і заощадити ресурси на етапі розробки. У юридичному

дизайні прототипом може бути оновлений варіант договору, полісу, інструкції чи іншого документа з новою структурою, спрощеним текстом, візуальними елементами та інфографікою. На цьому етапі допускаються недосконалості – головне отримати зворотний зв'язок і виявити, що працює добре, а що потребує доопрацювання. Створення прототипів дає змогу швидко реагувати на виявлені проблеми й адаптувати продукт до реальних потреб користувачів.

Приклад: намалювати на аркуші спрощену інфографіку процесу оформлення страхового випадку.

5. Тестування (Testing)

Тестування є критичним етапом у процесі юридичного дизайну, який дозволяє перевірити ефективність створеного прототипу на реальних користувачах. На цьому етапі виявляються слабкі місця документа або процесу: які частини залишаються незрозумілими, де користувачі відчують труднощі, чи відповідає кінцевий продукт очікуванням і потребам аудиторії. Тестування допомагає не лише виявити проблеми, а й зібрати цінний зворотний зв'язок, який стане основою для подальших удосконалень.



Процес тестування може включати інтерв'ювання, спостереження за взаємодією користувачів із прототипом, анкетування або організацію фокус-груп. Важливо не просто запитувати думку, а й аналізувати поведінку: де користувач вагається, де помиляється, де втрачає логіку або інтерес. У юридичному дизайні особливу увагу приділяють простоті сприйняття, швидкості розуміння змісту та загальному емоційному досвіду користувача.

Приклад: користувач не може швидко знайти інформацію про строки виплати страховки – це сигнал про потребу змінити структуру.

6. Удосконалення і впровадження (Iteration & Implementation)



Після проведення тестування настає етап удосконалення та впровадження. Удосконалення (ітерація) означає внесення змін до прототипу на основі отриманого зворотного зв'язку та виявлених недоліків. Команда аналізує результати тестування та працює над тим, щоб усунути непорозуміння, спростити складні елементи, підвищити інтуїтивність і загальну якість юридичного продукту. У юридичному дизайні ітерації можуть повторюватися кілька разів, доки не буде досягнуто оптимального балансу між зрозумілістю, точністю та ефективністю.

Після фінального доопрацювання продукт готовий до впровадження. Впровадження (Implementation) передбачає інтеграцію оновленого документа або процесу в реальне середовище. Це може бути оновлення внутрішньої документації компанії, запуск нової форми договору для клієнтів або адаптація юридичних інструкцій для ширшої аудиторії. Дуже важливо підготувати користувачів до змін – шляхом інформування, навчання або супровідних матеріалів. Успішне впровадження вимагає також організації підтримки користувачів і готовності до подальшого удосконалення продукту на основі реальної практики.

З корисними відео від Лабораторії юридичного дизайну можна ознайомитися за гіперпосиланням¹⁵⁰.



Також пропонується здійснити моніторинг вебсторінки Стенфордської лабораторії юридичного дизайну  [Stanford Legal Design Lab](https://law.stanford.edu/legal-design-lab/)¹⁵¹, яка

¹⁵⁰ Лабораторія юридичного дизайну. URL: <https://www.youtube.com/@legaldesignlab> (дата звернення: 18.05.2025).

¹⁵¹ Stanford Legal Design Lab. . URL: <https://law.stanford.edu/legal-design-lab/> (date of access: 17.05.2025).

містить інформацію про реалізовані та поточні проєкти у сфері юридичного дизайну, а також надає доступ до актуальних, змістовних і практично орієнтованих матеріалів з відповідної тематики.

Основні виклики юридичного дизайну

Виклик	Пояснення
Баланс між простотою і юридичною точністю	Важко спростити документ без втрати юридичної точності
Опір традиційних юристів	Юристи звикли писати складно і формально
Вартість розробки	Хороший юридичний дизайн потребує інвестицій часу і ресурсів
Оновлення законодавства	Зміни у праві змушують постійно оновлювати юридичні продукти

ПЕРЕВІРКА ЗНАНЬ

What is true and what is false? Justify your answer.

1. Концепція правового дизайну суперечить традиційним принципам юридичної точності, тому її не можна використовувати в офіційних документах.
2. Принцип «людиноцентричності» в правовому дизайні полягає в адаптації юридичного мислення до потреб і сприйняття кінцевого користувача.
3. Ідеація як етап правового дизайну передбачає формування одного найбільш правильного юридичного рішення без альтернатив.
4. Правовий дизайн може застосовуватись як у створенні нових юридичних інструментів, так і в переробці вже існуючих, які викликають складнощі у сприйнятті.
5. Правовий дизайн обмежується лише візуальними аспектами тексту, такими як шрифти та піктограми.
6. Прототипування дозволяє юристу побачити, як користувач взаємодіє з юридичним документом ще до його юридичного затвердження.

7. Методологія правового дизайну передбачає залучення кінцевого користувача лише на етапі тестування готового продукту.

8. Правовий дизайн є частиною ширшої концепції доступу до правосуддя, яка визнає, що складні юридичні тексти можуть фактично обмежувати права.

9. Успішний правовий дизайн виключає необхідність участі юристів у підготовці текстів – достатньо дизайнерів та UX-фахівців.

10. Тестування в юридичному дизайні – це суто технічна перевірка верстки документа, без участі користувачів.

ЗАВДАННЯ



1. Practical task

Оберіть будь який типовий договір (наприклад, оренди квартири або купівлі-продажу товару) і:

- *спростіть формулювання (перепишіть юридично грамотно, але простіше);*
- *розбийте текст на розділи з короткими назвами;*
- *додайте іконки або схеми для кращого сприйняття.*



2. Infographic “How to File a Lawsuit”

Створіть інфографіку для громадян, де крок за кроком буде пояснено процес подання позову:

- *які документи потрібні;*
- *куди звертатися;*
- *як відбувається реєстрація.*



3. Analysis of a legal document for usability

Використайте реальний юридичний документ (наприклад, банківський договір або умови страховки) і:

- *виділіть незрозумілі терміни;*

- оцініть текст за критеріями: зрозумілість, візуальна структура, доступність;
- запропонуйте три способи його покращення.



4. Legal designer

Формат: швидке завдання на час.

Перетворіть складний уривок з закону або договору у:

- коротке пояснення (до 5 речень),
- візуальну схему або блок-схему.



5. Understand me

Формат: робота в парах або командах.

Один студент отримує типовий юридичний документ і має пояснити іншому його суть максимально просто, без юридичної мови.

Другий студент оцінює: що залишилося незрозумілим.



6. Contract design of the future

Формат: творча робота.

Сформулюйте та візуалізуйте концепцію того, яким може бути формат та зміст договору через 10 років з урахуванням тенденцій цифровізації, юридичного дизайну та розвитку технологій:

- чи буде він повністю візуальний?
- якими будуть підписи?
- чи потрібно буде взагалі читати договір?

7. Questions for discussion

1. Чи потрібно спрощувати всі юридичні документи, чи лише певні категорії?
2. Чи може юридичний дизайн знизити кількість судових спорів?
3. Як знайти межу між простою мовою і юридичною точністю?

4. Чи варто зобов'язати державні органи використовувати юридичний дизайн у публічних документах?

5. Які навички юриста майбутнього будуть критично важливими у світі юридичного дизайну?



8. Topics for presentations

1. Юридичний дизайн: новий підхід до правової комунікації.
2. Історія розвитку юридичного дизайну: від візуалізації права до інтерактивних контрактів.
3. Візуальні договори: переваги та ризики.
4. Юридичний дизайн у сфері захисту прав споживачів.
5. Дизайн-мислення і право: точки перетину.
6. Перспективи впровадження юридичного дизайну у державних послугах.
7. Юридичний дизайн в епоху штучного інтелекту: виклики та можливості.

Розділ X ПРОВОВА ІНФОРМАТИКА

LEGAL INFORMATICS

1. Теоретичні основи правової інформатики

У процесі свого існування та розвитку людство пройшло через низку етапів, на кожному з яких рівень життя залежав від компетентності у роботі з інформацією. Аграрний та індустріальний періоди змінилися інформаційною епохою, в якій головною рушійною силою стали інформація, дані та знання. У сучасному світі – це суспільство знань і глобальної компетентності, яке висуває нові вимоги до професійної підготовки. Щоб бути конкурентним у XXI столітті, фахівець має володіти такими ключовими навичками:



Здатність до критичного мислення



Універсальні, системні знання



Компетенції в галузі ІКТ



Здатність до прийняття рішень



Управління динамічними процесами



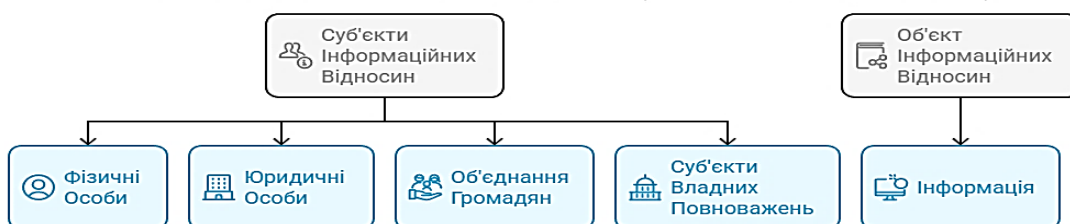
Уміння працювати в команді



Уміння налагоджувати комунікацію

Згідно зі ст. 1 Закону України «Про інформацію», інформація визначається як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»¹⁵².

Суб'єкти і об'єкт інформаційних відносин (ст. 4 ЗУ "Про інформацію")



Стаття 17. Правова інформація¹:

1. **Правова інформація** – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. **Джерелами правової інформації** є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення медіа, публічні виступи, інші джерела інформації з правових питань.

¹⁵² Про інформацію: Закон України від 02.10.1992 № 2657-XII: станом на 15 листопада 2024 р.
URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 26.03.2025).

Правова інформатика як наука вивчає закономірності створення, обробки, зберігання та використання інформації в правовій сфері. Її теоретичні основи базуються на синтезі знань із права, інформатики та теорії управління. Центральним об'єктом дослідження є правова інформація, яка має відповідати таким властивостям, як:

Нормативність	Правова інформація має офіційний характер і підкріплена державним примусом (норми права, закони, підзаконні акти), що відрізняє її від інформації загального характеру.
Достовірність	Юридична сила правової інформації залежить від її відповідності дійсному стану речей.
Системність	Правова інформація повинна мати чітку ієрархію (Конституція → закони → підзаконні акти) та логічні зв'язки між різними джерелами права.
Актуальність	Через постійні зміни в законодавстві правова інформація потребує регулярного оновлення.
Доступність	Правова інформація має бути відкритою для громадян (за винятком конфіденційних або секретних даних).
Формальна визначеність	Правова інформація має строго визначену форму і суворі реквізити, відсутність яких може зробити її недійсною.
Захищеність	Правова інформація має бути захищеною від несанкціонованого доступу, витоку та маніпуляцій у зв'язку з конфіденційністю даних (особисті дані, комерційна таємниця тощо).

Однією з ключових категорій правової інформатики є **інформаційні процеси**, які дозволяють оптимізувати роботу юристів, правоохоронних органів та державних установ, зменшуючи часові витрати та ризики помилок, пов'язаних із ручною обробкою даних.



Важливим аспектом інформаційних процесів у правовій сфері є **обробка та аналіз великих масивів юридичних даних**. Завдяки сучасним технологіям, таким як ІІІ і машинне навчання, можна автоматизувати аналіз судових рішень, виявляти закономірності в правозастосуванні та прогнозувати результати справ.

Окремим напрямом дослідження є **правове регулювання інформаційних процесів**, яке визначає правила їх функціонування в юридичній сфері. До таких процесів належать стандарти електронного документообігу, вимоги до захисту даних у державних реєстрах, процедури надання електронних послуг у сфері правосуддя. Національне та міжнародне законодавство (наприклад, Загальний регламент захисту даних Європейського Союзу (GDPR)¹⁵³ в ЄС або Закон України «Про електронні документи та електронний документообіг»¹⁵⁴) встановлюють правові рамки для збору, обробки та зберігання інформації, гарантуючи її легітимність і безпеку. Це забезпечує баланс між технологічними можливостями та правами громадян на конфіденційність і захист персональних даних.

Отже, правова інформатика є ключовим інструментом підвищення ефективності та прозорості правозастосування в умовах цифрової трансформації суспільства.

¹⁵³ Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європ. Союзу від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 28.03.2025).

¹⁵⁴ Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення: 28.03.2025).

2. Інформаційна безпека в юридичній діяльності

Одним із ключових напрямків правової інформатики є дослідження **інформаційної безпеки**, яка набуває особливого значення в умовах цифровізації юридичних процесів. Сюди входять не лише технічні аспекти захисту даних, але й правові механізми, що регулюють обіг інформації, зокрема персональних даних, конфіденційних документів і службових таємниць.

На сьогодні, в українському законодавстві відсутнє трактування терміну «інформаційна безпека», однак, В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. пропонують авторське визначення:

«**Інформаційна безпека** – це стан захищеності життєво важливих інтересів особи, суспільства та держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, моральноетичний тощо), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди»¹⁵⁵.



Досить часто, поряд з терміном «інформаційна безпека», розглядають і поняття «кібербезпека». Законом України «Про основні засади кібербезпеки України» визначено, що «**Кібербезпека** – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі»¹⁵⁶.

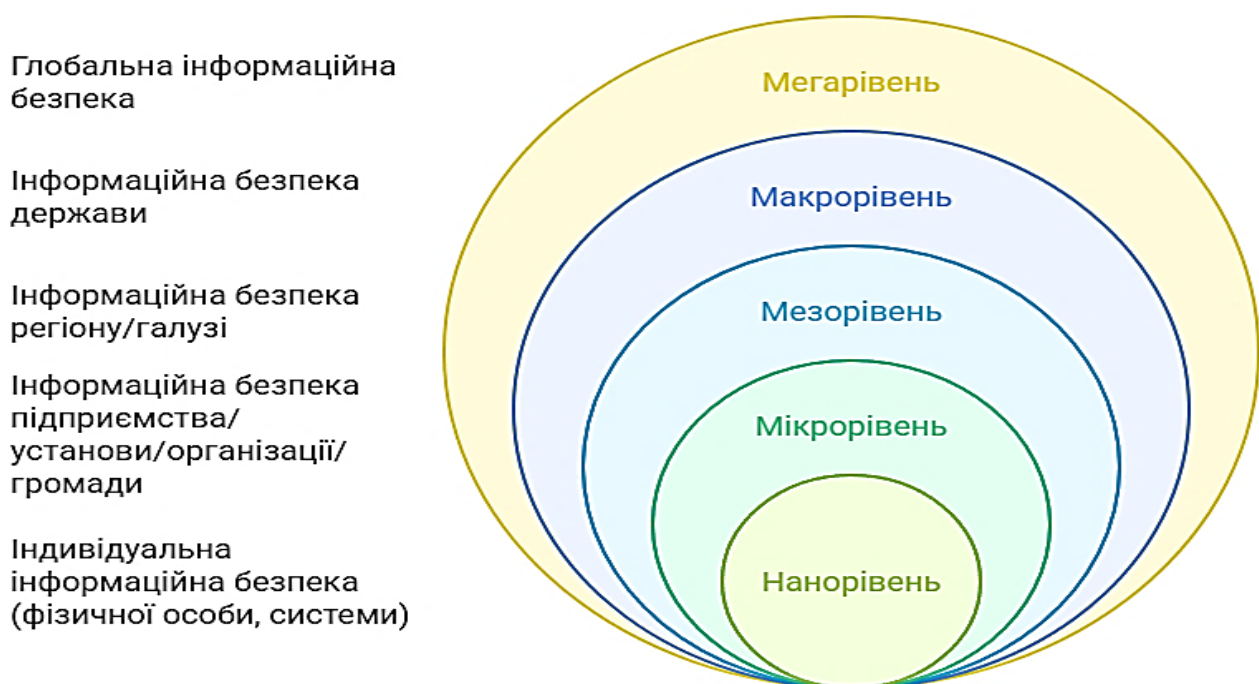
Інформаційна безпека як комплексний понятійний конструкт охоплює захист даних, інформаційних систем і комунікацій від будь-яких загроз, тоді як

¹⁵⁵ Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

¹⁵⁶ Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 28.03.2025).

кібербезпека є її технологічною складовою, зосередженою на протидії кіберзагрозам у цифровому середовищі. Однак у сучасних умовах глобалізації та цифровізації ці категорії набувають особливого значення на макрорівні – коли мова йде про інформаційну безпеку держави. Вона передбачає не лише захист критичної інфраструктури від кібератак, а й стратегічне управління інформаційними потоками, протидію гібридним загрозам (зокрема, дезінформації) та забезпечення національного суверенітету в інформаційному просторі.

Рівні інформаційної безпеки



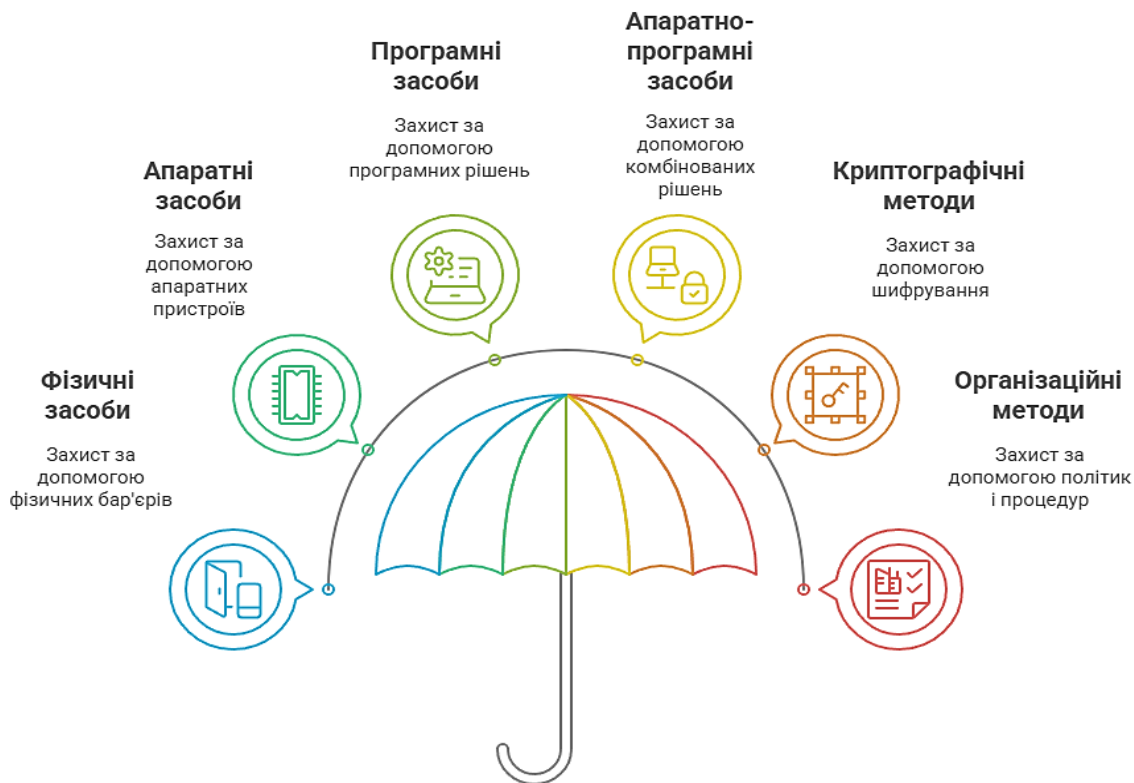
«Інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом»¹⁵⁷.

¹⁵⁷ Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 28.04.2025).

Важливим елементом інформаційної безпеки є **захист персональних даних**, особливо в контексті юридичної діяльності, де обробляється великий обсяг конфіденційної інформації. В Україні цей аспект регулюється Законом «Про захист персональних даних»¹⁵⁸, а також нормами GDPR для взаємодії з ЄС. Порушення цих вимог може призвести до серйозних правових наслідків, включаючи штрафи та позови від клієнтів.

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Методи захисту інформації

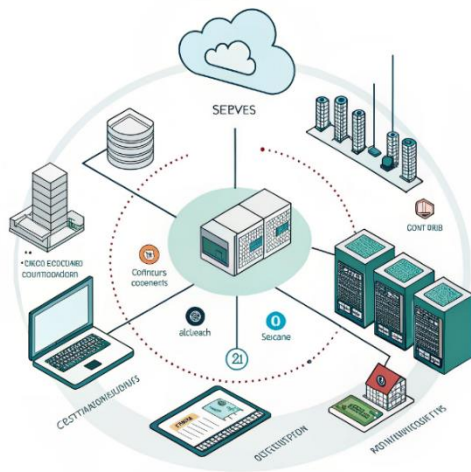


Окрему увагу приділяють **захисту інформації** у правових процесах. Через високі вимоги до конфіденційності та цілісності даних використовуються методи криптографії, електронні цифрові підписи (ЕЦП) та печатки, систем контролю доступу та запобігання кібератакам. Особливо це стосується е-документообігу, де необхідно забезпечити автентичність документів і захист персональних даних.

¹⁵⁸ Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 28.03.2025).

3. Хмарні технології у юридичній діяльності

У сучасних умовах розвитку інформаційного суспільства важливим інструментом забезпечення ефективної юридичної практики є хмарні технології. Вони дозволяють юристам оперативно здійснювати обробку, зберігання та обмін правовою інформацією, дотримуючись вимог безпеки та конфіденційності даних.



Хмарні технології – це модель надання обчислювальних ресурсів (серверів, сховищ даних, додатків, мереж тощо) через Інтернет на умовах гнучкого використання без необхідності фізичного управління інфраструктурою. У межах юридичної діяльності хмарні сервіси використовуються для зберігання правових документів, спільної роботи над справами, організації дистанційного правосуддя та оптимізації документообігу.

Переваги хмарних технологій для юристів



Проте, разом із перевагами, застосування хмарних технологій вимагає врахування специфічних **правових аспектів**. Зокрема, зберігання конфіденційної інформації клієнтів у хмарних середовищах має відповідати нормам законодавства щодо захисту персональних даних, таким як GDPR та Закон України «Про захист персональних даних». Вибір постачальника хмарних послуг має базуватися на оцінці його здатності забезпечити необхідний рівень безпеки і правової захищеності інформації, включаючи укладення договорів про обробку персональних даних.

Ризики хмарних технологій



Для мінімізації цих ризиків необхідно впроваджувати внутрішні політики інформаційної безпеки, здійснювати регулярний аудит постачальників хмарних послуг, використовувати засоби шифрування даних та навчати співробітників правилам безпечного поводження з інформацією.

На практиці юристи активно використовують такі хмарні сервіси як **Google Workspace**, **Microsoft 365**, а також спеціалізовані платформи для юридичної практики, що забезпечують можливості управління справами, електронного документообігу, організації відеозустрічей та обліку робочого часу.

Стаття 3. Види хмарних послуг¹⁵⁹

2. До хмарних послуг належать:

інфраструктура як послуга – хмарна послуга, що полягає у наданні користувачу хмарних послуг обчислювальних ресурсів, ресурсів зберігання або систем електронних комунікацій за допомогою технології хмарних обчислень;

платформа як послуга – хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до інфраструктури та наборів комп'ютерних програм (операційних систем, системних комп'ютерних програм, програмних засобів для комп'ютерного програмування, програмних засобів управління базами даних) за допомогою технології хмарних обчислень;

програмне забезпечення як послуга – хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до прикладних комп'ютерних програм за допомогою технології хмарних обчислень через онлайн-сервіс або комп'ютерні програми-агенти;

безпека як послуга – послуга з кіберзахисту, що надається користувачу хмарних послуг з використанням хмарних ресурсів;

інші послуги, що відповідають визначенню хмарних послуг.

Таким чином, хмарні технології є невід'ємною складовою цифровізації юридичної діяльності. Їх правильне використання дозволяє підвищити ефективність роботи юридичних фахівців, забезпечити збереження інформації та відповідність сучасним вимогам правового регулювання інформаційних процесів.

¹⁵⁹ Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX : станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення: 28.04.2025).

Перспективи розвитку хмарних технологій в юридичній сфері



4. Автоматизація роботи з юридичними документами

Текст є основним видом інформації, з яким працюють юристи під час підготовки, аналізу та обміну правовими документами в електронному середовищі. Тому так важливо грамотно створювати, формувати та структуровано оформлювати юридичні тексти. Для опрацювання текстових даних застосовують три основні класи прикладного програмного забезпечення: **текстові редактори, текстові процесори та видавничі системи.**

Текстовий редактор – прикладний застосунок, призначений виконувати операції над текстом, серед яких: створення текстового електронного текстового документа, редагування тексту (внесення правок), перегляд вмісту документа на екрані та його друк.

Головною перевагою текстових редакторів є те, що всі вони працюють з текстом однаково, а тому введений текст в одному текстовому редакторі можна редагувати в інших без особливих труднощів. До текстових редакторів, сумісних із ОС Windows відносять: *Блокнот*; *WordPad*; *Bred 3.0.3*; *Leafpad* та ін.

Текстові редактори, що мають ширший спектр можливостей для роботи з текстом отримали назву **текстовий процесор** (Рис. 1). Текстові процесори слугують для роботи з великими документами та/або тоді, коли тексту потрібно надати зовнішній вигляд та/або додати нетекстові об'єкти.



Рис. 1. Функції текстового процесора

На відміну від текстових редакторів, перенесення тексту з одного текстового процесору до іншого не завжди можливе, а дані переносяться без збереження форматування. До текстових процесорів, які функціонують на базі ОС Windows відносять: *Microsoft Word*; *LibreOffice Writer*; *OpenOffice Writer*; *AbiWord*; *Corel WordPerfect*; *KWord* та ін.

Для потреб поліграфічної галузі використовуються видавничі системи, що представляють апаратно-програмний комплекс для підготовки і тиражування друкарської продукції та є одним із елементів видавничої справи.



Microsoft Office Word – багатфункціональний текстовий процесор, що входить до пакета прикладних програм *Microsoft Office*, основними перевагами якого є: простий та зручний інтерфейс;

створення текстових документів будь-якої складності; можливість форматування тексту; робота із нетекстовими об'єктами; інтеграція з іншими програмами, що входять до офісного пакету; перевірка правопису та інтелектуальний аналіз тексту; створення шаблонів документів та робота з макросами тощо.

Запустити текстовий процесор можна кількома способами, серед яких: через меню «Пуск»; через закріплений значок на «Панелі завдань»; через подвійне натискання ярлика програми на робочому столі. Після запуску, користувач має змогу бачити стандартне для додатків *MS Office* програмне вікно (Рис. 2).

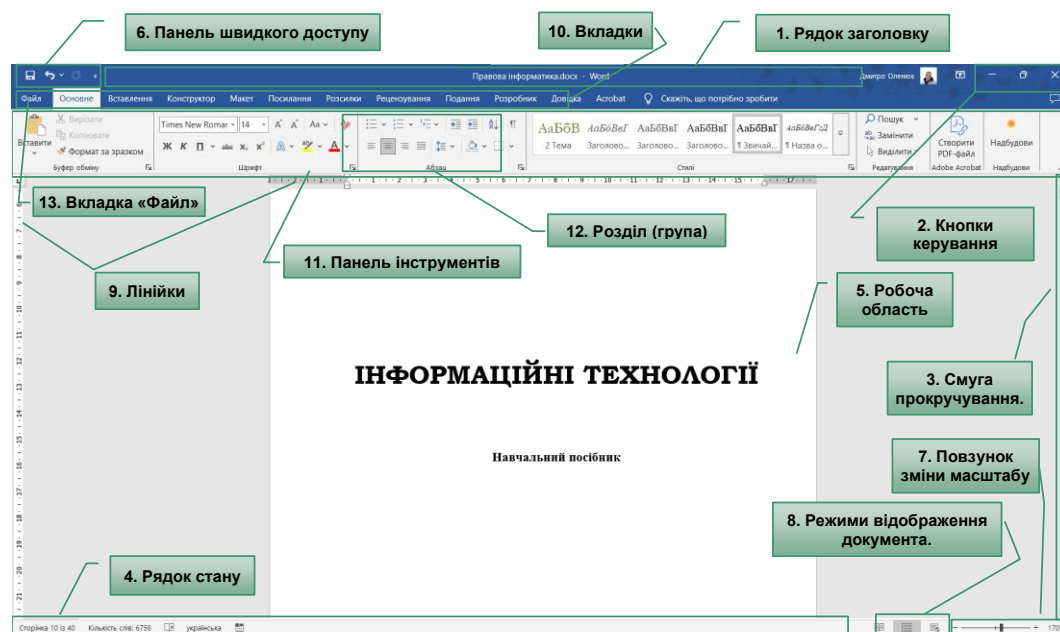


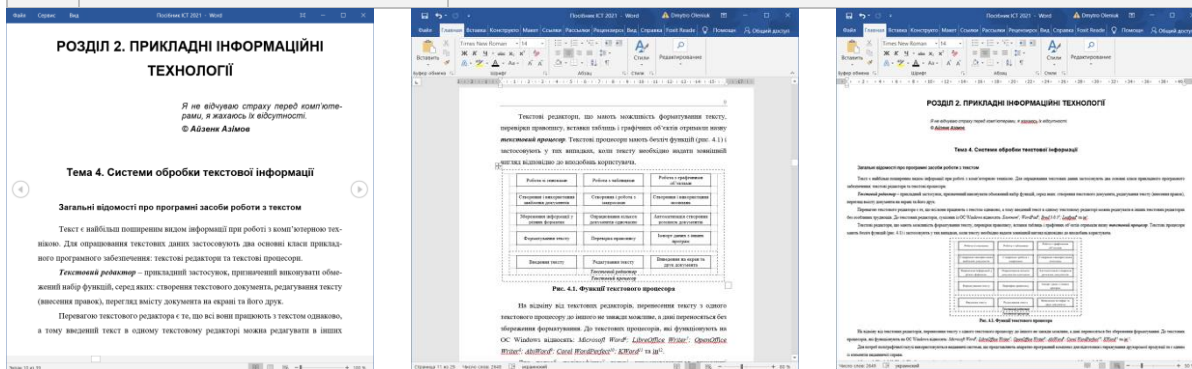
Рис. 2. Вікно текстового процесора MS Word

Основні елементи інтерфейсу та їх коротка характеристика наведено у табл. 1.

Таблиця 1 – Елементи інтерфейсу MS Word

№ з/п	Елемент інтерфейсу	Коротка характеристика
1.	Рядок заголовку	Розміщений у верхній частині вікна програми та містить відомості про назву (ім'я) документа.
2.	Кнопки керування вікном	– згорнути вікно; – зміна розміру вікна (згортання і розгортання); – закрити вікно.
3.	Смуга прокручування	Дозволяє переміщуватись по документу для відображення інформації, яка не вміщується у відведеному для неї місці на екрані.

4.	Рядок стану	Відображає відомості про стан документа: поточну сторінку, загальну кількість сторінок у документі, кількість слів, мову введеного тексту та ін.
	Робоча область	Призначена для відображення поточного документа з яким працює користувач.
5.	Панель швидкого доступу	Призначена для швидкого і зручного доступу до інструментів та команд, у яких найчастіше виникає потреба.
6.	Повзунок зміни масштабу	Призначений для збільшення або зменшення масштабу відображення документа у робочому вікні.
7.	Режими відображення документа (Рис. 3)	 – режим читання (панелі інструментів приховуються для зручності перегляду вмісту документа);  – режим сторінки (для редагування та форматування вмісту документа);  – режим «веб-документ» (для перегляду документа у форматі веб-сторінки).
8.	Лінійки	Містять маркери () для зміни значень деяких властивостей у документі (розмір поля, абзацний відступ тощо).
9.	Вкладки	Назви стрічок, які об'єднують командні кнопки за функціональним принципом («Головна», «Вставка», «Конструктор», «Макет» та ін.)
10.	Панель інструментів	Містить кнопки команд для виконання певних дій при роботі з документом
11.	Розділ (група)	Розділи об'єднують інструменти за їх функціональними можливостями, наприклад: Шрифт – інструменти для роботи із шрифтами (тип, розмір, колір та ін.).
12.	Вкладка «Файл»	Містить набір інструментів для роботи з файлами документів такі, як: «Відомості», «Створити», «Відкрити», «Зберегти», «Зберегти як», «Друк» та ін.



Режим читання

Режим сторінки

Режим «веб-документ»

Рис. 3. Режими відображення документа

Налаштування параметрів роботи програми.

Для налаштування інтерфейсу необхідно перейти до вкладки **Файл** та обрати опцію **Більше** – **Параметри** (Рис. 4). У вікні, що з'явиться (Рис. 5) можна здійснювати наступні налаштування: **Загальні**, **Відображення**, **Правопис**, **Збереження**, **Мова**, **Спеціальні можливості**, **Додатково**, а також налаштування **Стрічки**, **Панелі швидкого доступу**, **Надбудов** та **Центру управління безпекою**.

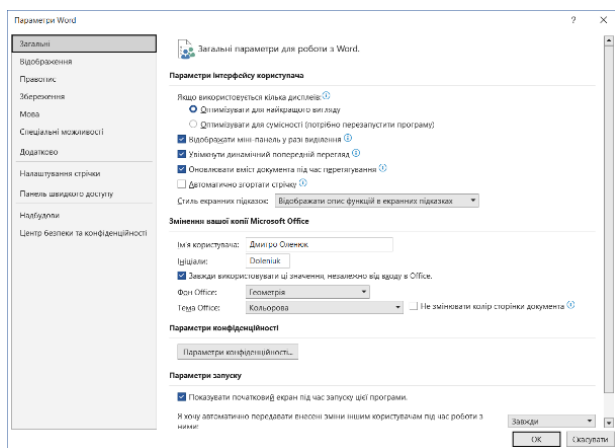
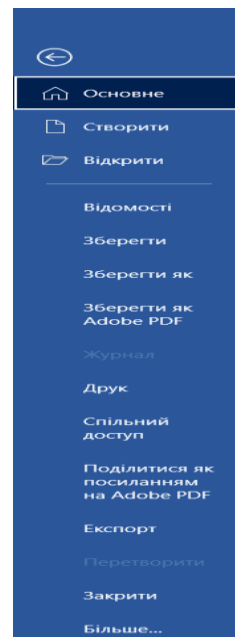


Рис. 5

Особисте

налаштування *Microsoft Office*, із вказанням *Рис. 4* користувача (власника документів) здійснюється при першому встановленні офісного пакета на комп'ютер. Для цього необхідно мати обліковий запис *Microsoft* та під'єднання до глобальної мережі *Internet*.



Робота з документами.

Робота з документами полягає у виконанні із ними певних операцій, таких, як: створення нового документа, збереження, створення резервної копії, відкриття файлів, попередній перегляд документа.

Word дозволяє створити новий документ двох видів: пустий або на основі шаблону. Для цього: Відкрийте *Word* (Рис. 6) або **Файл** → **Створити** та виберіть опцію «Пустий документ» чи будь-який із запропонованих шаблонів.

Для того, щоб вперше зберегти документ потрібно

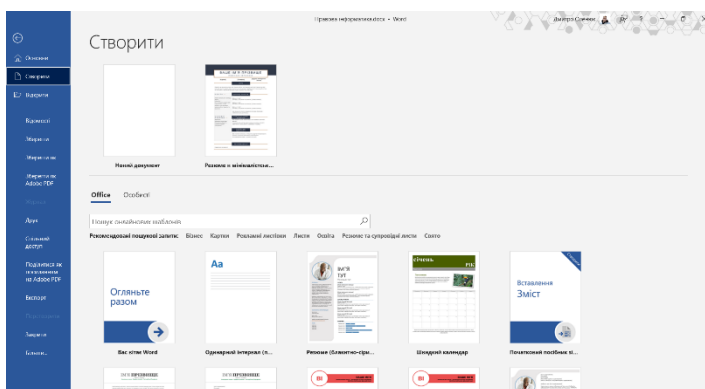


Рис. 6.

виконати наступну послідовність дій: **Файл** → **Зберегти документ як** → обрати папку, де буде збережено документ → у вікні, що з'явиться дати назву та вказати

тип файлу → натиснути «ОК». Після того, як файл було збережено вперше, користувач може продовжувати роботу із документом, а у разі потреби зберегти зміни потрібно клацнути **Файл → Зберегти** або скористатися комбінацією клавіш **Ctrl + S** або клацнути на символ , який знаходиться на панелі швидкого доступу.

Якщо користувач працює із документом тривалий час, доцільно налаштувати створення резервної копії файлу, для цього: натисніть на вкладку **Файл → Параметри → Збереження → Автозбереження** (Рис. 7) і задати час, через який створюватиметься резервна копія документа.

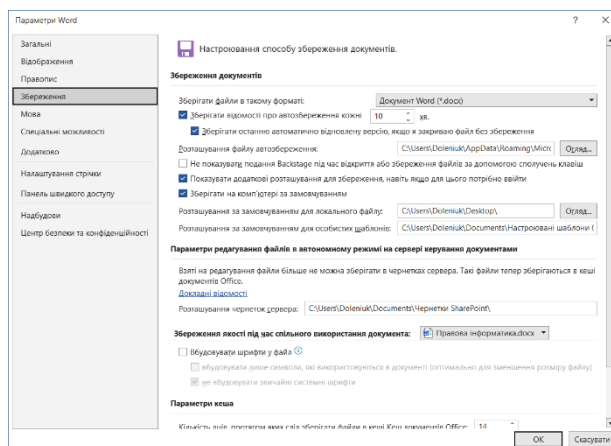


Рис. 7.

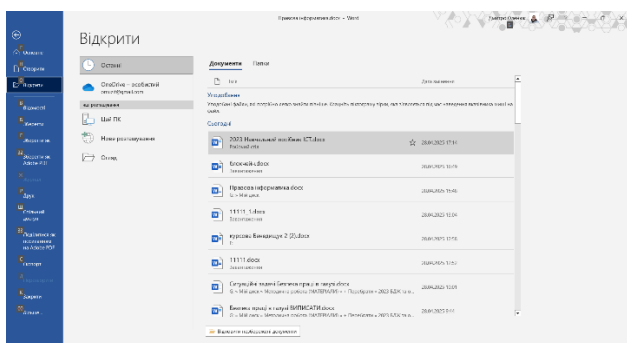


Рис. 8.

Для того, аби розпочати роботу із новим документом, не закриваючи при цьому поточний, необхідно: натиснути **Файл → Відкрити → обрати потрібний документ із останніх**, або той, який зберігається на комп'ютері чи

електронному носії (Рис. 8) або скористатися комбінація клавіш **Ctrl + O**.

Попередній перегляд документа здійснюється наступним чином: **Файл → Друк** або скористатися комбінацією клавіш **Ctrl+P** (Рис. 9).

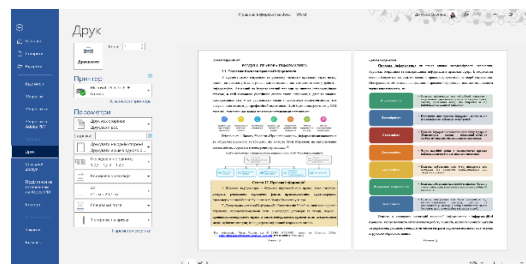
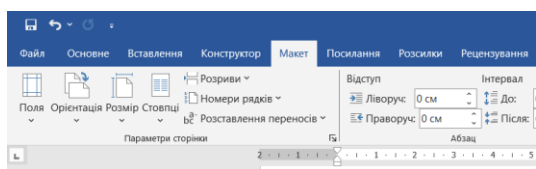


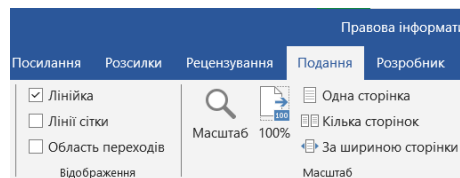
Рис. 9.

Налаштування параметрів сторінки.

Налаштувати параметри сторінки можна безпосередньо на вкладці **Макет → група Параметри сторінки** (Рис. 10.а), або подвійним натисканням на форматну лінійку або пересуванням меж на самій лінійці. Для того, щоб увімкнути форматну лінійку, потрібно перейти на вкладку **Подання → група Відображення** та поставити маркер навпроти **Лінійки** (Рис. 10.б).



а)



б)

Рис. 10.

У діалоговому вікні **Параметри сторінки** (Рис. 11) користувач може задати розмір полів, орієнтацію сторінки, розмір сторінки тощо.

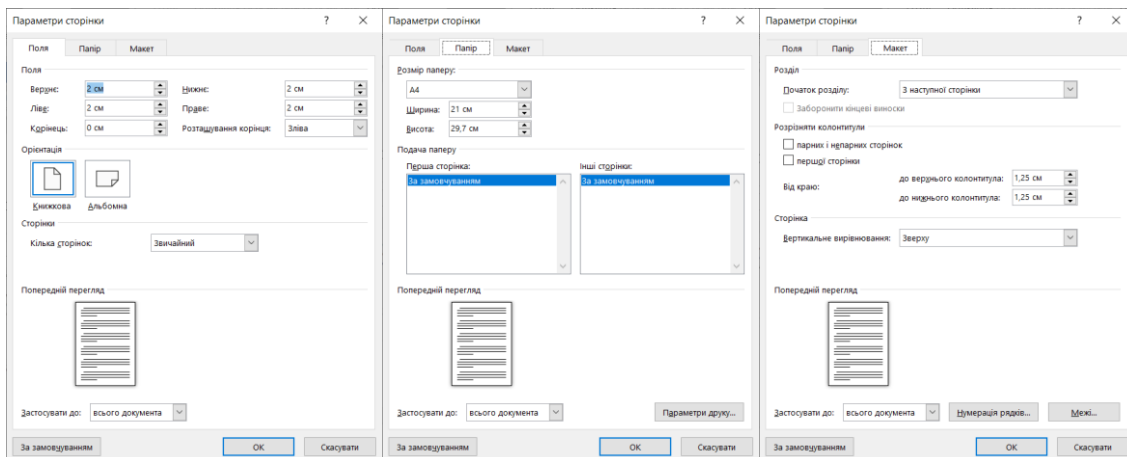


Рис. 11.

Якщо на сторінці потрібно встановити фон або границі, для цього потрібно перейти на вкладку **Конструктор** → група **Фон сторінки** і скористатися одним із доступних там інструментів (Рис. 12).

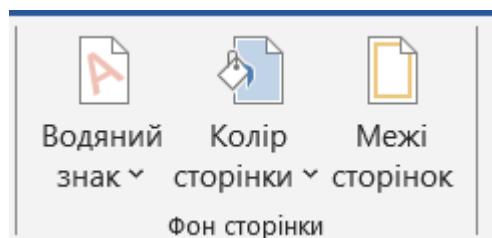


Рис. 12.

Колонтитули.

Колонтитул – особлива частина документа, яка містить заголовкові дані. У колонтитулах також розміщують назву документа та/або його частини, глави, параграфа, нумерацію сторінок тощо. Розрізняють верхній та нижній колонтитул.

Користувач має змогу налаштувати колонтитул відповідно до власних потреб, у тому числі: розміщувати інформацію, яка буде різною на парних і непарних сторінках документа, задати особливий колонтитул для першої сторінки, наприклад, коли потрібно пронумерувати сторінки документа починаючи з другої тощо.

Для того, щоб редагувати колонтитули, необхідно двічі натиснути на верхнє або нижнє поле будь-якої сторінки документа, після чого з'явиться додаткова вкладка «Конструктор – робота з колонтитулами» (Рис. 13).

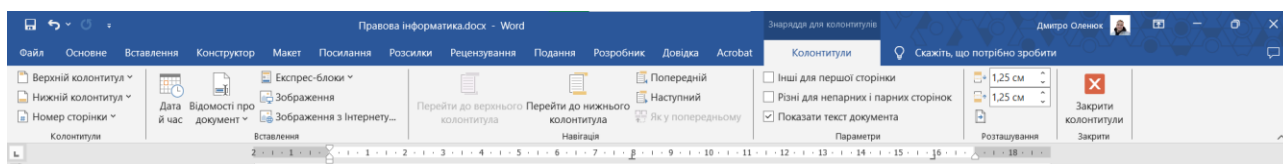


Рис. 13.

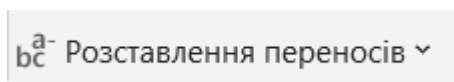
Базові прийоми роботи з текстом.

Введення тексту відбувається у вікні документа на його робочій області у тому місці, де знаходиться курсор. Word дає змогу вільно вводити текст, для цього потрібно двічі клацнути у будь-якому порожньому місці робочої області.

Мова введення. Для зміни мови введення тексту можна скористатися такими комбінаціями клавіш **Ctrl + Shift** або **Alt + Shift** або клацнути по індикатору мови на панелі задач і обрати потрібну із списку.

Зміна регістра. Для зміни регістру потрібно затиснути клавішу **Shift**, якщо це одноразово (наприклад, введення слова із великої літери «Україна») або натиснути **CapsLock**, для введення тексту верхнім регістром (наприклад, для введення аббревіатури «ЖОДА» – Житомирська обласна державна адміністрація). Повторне натискання даних клавіш змінює регістр з малих літер на великі, і навпаки (наприклад, «логіка → Логіка → ЛОГІКА → Логіка → логіка»).

Автоматичне перенесення слів. Для ввімкнення автоматичного перенесення слів оберіть вкладку **Макет** → група **Параметри сторінки** →



Під час редагування документа використовують недруковані символи (табл. 2). Для їх відображення на екрані, необхідно натиснути на символ «¶», який знаходиться у групі **Абзац** вкладки **Головна**.

Таблиця 2. – Недруковані символи

№ з/п	Недрукований символ	Клавіші введення	Позначення
1.	Пропуск	Пробіл	•

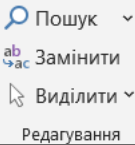
2.	Нерозривний пропуск	Ctrl + Shift + пробіл	°
3.	Кінець абзацу	Enter	
4.	Табуляція	Tab	→
5.	М'який перенос	Ctrl + дефіс	
6.	Нерозривний дефіс	Ctrl + Shift + дефіс	—
7.	Розрив рядка	Shift + Enter	
8.	Розрив сторінки	Ctrl + Enter	Разрыв страницы

Переміщення по документу здійснюється за допомогою миші або клавіш керування курсором (←, ↑, →, ↓; **Ctrl** + ←/↑/→/↓), а також клавішами **Ctrl** + **PageUp**, **Ctrl** + **PageDown**, **Ctrl** + **Home**, **Ctrl** + **End**.

Якщо користувачем було допущено помилку та існує потреба повернутися на крок назад, тоді доцільно скористатися клавішею , яка знаходиться на панелі швидкого доступу або комбінацією клавіш **Ctrl** + **Z**.

Основні операції із фрагментами тексту наведено у табл. 3.

Таблиця 3. – Операції над фрагментами тексту

№ з/п	Назва операції	Способи реалізації
1.	Виділення	Виділення фрагмента тексту мишею або із використанням клавіш керування курсором (Shift + ←/↑/→/↓). Виділення всього документа Ctrl + A .
2.	Вилучення	Виділений фрагмент вилучають із використанням клавіш Delete або Backspace ;
3.	Копіювання	Виділений фрагмент копіюють із використанням комбінації клавіш Ctrl + C або клацнувши на піктограму  Копіювати (Вкладка Головна → група Буфер обміну)
4.	Вставка	Вставити фрагмент тексту можна комбінацією клавіш Ctrl + V або клацнувши на піктограму  Вставити (Вкладка Головна → група Буфер обміну)
5.	Вирізання	Вирізати фрагмент тексту можна комбінацією клавіш Ctrl + X або клацнувши на піктограму  Вирізати (Вкладка Головна → група Буфер обміну)
6.	Пошук та заміна	Вкладка Головна → група Редагування 

Правопис слів та орфографія.

Для того, щоб користувач міг перевірити свій документ на наявність орфографічних помилок, неправильно введене слово буде підкреслене червоною хвилястою лінією (наприклад, Солво із помиклою).

Для ввімкнення автоматичної перевірки документа на наявність орфографічних помилок потрібно натиснути на вкладку **Файл** → **Параметри** → **Правопис** → **Автоматично перевіряти орфографію** → **ОК** (Рис. 14).

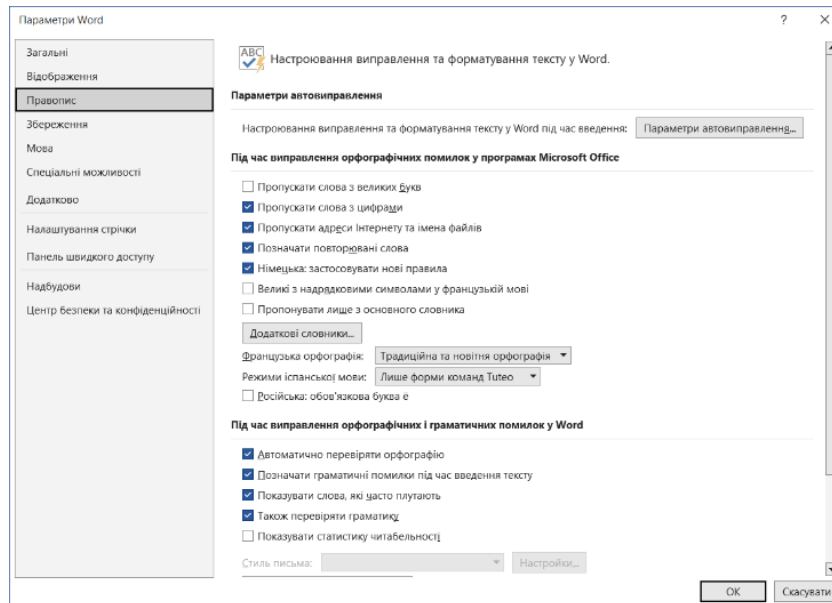


Рис. 14

Перевірка орфографії «вручну» здійснюється за наступним алгоритмом:

вкладка **Рецензування** → група **Правопис** →  **Правописання**.

Вставлення в текст спеціальних символів і автотексту.

Для того, щоб вставити у документ символ, потрібно розмістити курсор у потрібне місце та обрати вкладку **Вставка** → група **Символи** →  **Символ** (Рис. 15, 16).

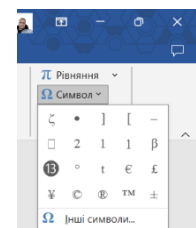


Рис. 15.

Автотекст – функція текстового процесора, яка скорочує час на введення найчастіше повторюваних у тексті слів. Наприклад, у тексті про систему освіти, слово «освіта» часто повторюватиметься, тому для того, щоб скористатися функцією **Автотекст**, потрібно виділити слово «освіта» і на вкладці **Вставка** → група **Текст** → піктограма  додати його до колекції, після

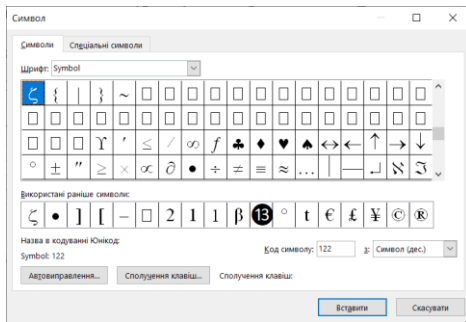


Рис. 16.

цього достатньо ввести літеру «о» та натиснути клавішу **F3**, щоб потрібне нам слово з'явилося на екрані.

Форматування.

У програмі MS Word, як і в будь-яких інших

текстових процесорах, для створення документа

використовують три складові: символи, абзаци та розділи. Електронний документ має наступну ієрархічну структуру:

1) **розділ** – частина документу, яка складається з одного або кількох абзацив, у більшості документів є тільки один розділ;

2) **абзац** – частина документу, яка складається з одного або кількох символів;

3) **символ** – найменший елемент документу (літера, цифра тощо).

Для кожного з цих складових використовуються свої атрибути форматування. Тобто в WORD застосовується трьохрівнева ієрархія форматування документа. **Форматуванням** називають процес зміни зовнішнього вигляду усього документа або його частини, тобто надання йому певного формату. Існує два способи форматування документу: до набору тексту та після набору тексту.

Кожен символ у документі WORD несе в собі інформацію про форматування, а саме:

- **Шрифт** – гарнітура символу.
- **Розмір** – визначає величину символу.
- **Накреслення** – Звичайний, напівжирний, Курсив, напівжирний курсив.
- **Підкреслення** – ні, Одинарне, Тільки слова, Подвійне чи Пунктирне.
- **Колір** – вибір кольору шрифту.
- **Ефекти** – Закреслений, Верхній індекс, Нижній індекс, Малі прописні, Усі прописні.
- **Інтервал** – визначає відстань між символами.
- **Зсув** – дозволяє підняти чи опустити символ щодо опорної лінії.

- *Кернинг* – відстань між визначеними парами букв.

Для форматування символів до набору тексту потрібно:

1. Ввести текст до того місця, поки не буде потрібно застосувати нове форматування.

2. Обрати необхідний новий формат для символів (тип шрифту, розмір, накреслення і т.д.), для цього можна скористатися відповідними кнопками панелі інструментів, чи командою *Формат → Шрифт*.

3. Продовжити набір тексту. Обраний формат буде застосовуватися до тексту, що набирається.

Для форматування символів після набору тексту потрібно:

1. Виділити текст, до якого потрібно застосовувати спеціальне форматування.

2. Вибрати необхідний формат (як в попередньому випадку).

В абзаці може бути багато символів, один чи взагалі жодного. При кожному натисканні [Enter] у текст поміщається мітка кінця абзацу і створюється новий абзац. Розуміння того, як WORD форматує абзаци, є ключовим в освоєнні принципів роботи WORD. Вся інформація про форматування абзацу міститься в мітці кінця абзацу (¶), тобто такі параметри форматування як (відступи, міжрядковий інтервал, позиції табуляції й інші) зберігаються в мітці кінця абзацу. Крім того, у ній зберігається і формат символу абзацу за замовчуванням.

Операції вирівнювання і форматування абзацу призначені для зміни зовнішнього вигляду абзацу. Текст вирівнюють по горизонталі і розташовують його між правим і лівим полем сторінки. У WORD застосовують 4 види вирівнювання абзацу: *по лівому краю* – усі рядки лівого краю абзацу утворюють вертикальну лінію; *по правому краю* – усі рядки правого краю абзацу утворюють вертикальну лінію; *по центру рядка* – розташовуються симетрично щодо вертикальної осі, що проходить через середину сторінки; *по ширині* – рівними виявляються і ліва і права границя.

До розділів застосовується найвищий рівень форматування документів WORD, що включає наступні параметри: розмір паперу; ліве, праве, верхнє і нижнє поля; орієнтація паперу: книжкова, альбомна; інформація про верхні і

нижні колонтитули; нумерація сторінок; нумерація рядків; кількість колонок і відстань між ними тощо. Як і для форматування абзаців, для форматування розділів використовується мітка кінця розділу (Розрив розділу (з наступної сторінки)). Якщо документ містить один розділ, він не містить мітки кінця розділу. Передбачається, що вона міститься наприкінці документа.

Якщо окремі сторінки треба відформатувати інакше (параметри форматування розділів перераховані нижче) варто розбити документ на кілька розділів, кожний з яких буде мати свій власний формат сторінок. WORD не має універсальної команди **Формат** → **Розділ**, яка відкривала би діалогове вікно для форматування розділів.

Зміна зовнішнього вигляду тексту відбувається із використанням інструментів, які знаходяться на вкладці **Головна** групи **Шрифт** (Рис. 17).

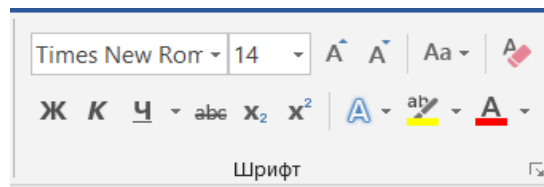
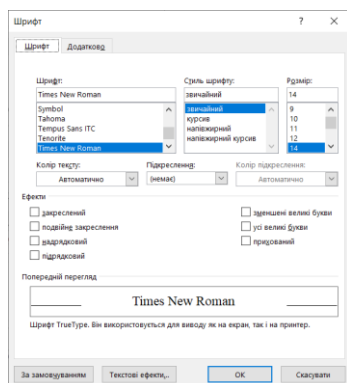
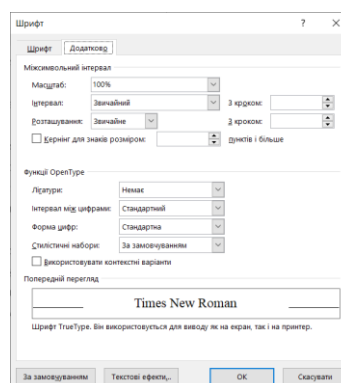


Рис. 17.

У діалоговому вікні групи **Шрифт** (Рис. 18.а) користувач має змогу налаштувати тип шрифту, його накреслення та розмір, а також колір, видозмінити його та додати текстові ефекти. На вкладці **Додатково** діалогового вікна **Шрифт** (Рис. 18.б) можна задавати міжсимвольний інтервал (масштаб тексту, інтервал між символами та зміщення). В даних даному діалоговому вікні є місце, яке показує той вигляд символів, який буде застосований до тексту після натискання користувачем кнопки «ОК».



а)



б)

Рис. 18.

Для більш зручного читання тексту, його можна вирівнювати відносно полів документа. Для цього потрібно перейти на вкладку **Головна** → група **Абзац** і скористатися одним із запропонованих варіантів (Рис. 19): по лівому краю; по центру; по правому краю; по ширині.

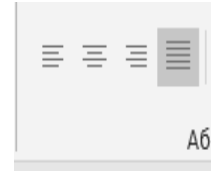


Рис. 19.

При форматуванні документа, не менш важливу роль для зовнішнього вигляду тексту відіграє міжрядковий та інтервал між абзацами. Щоб здійснити налаштування інтервалу, потрібно перейти до вкладки **Головна** та у групі **Абзац** викликати контекстне меню (Рис. 20). У цьому ж вікні можна здійснити налаштування відступів тексту та абзацного відступу.

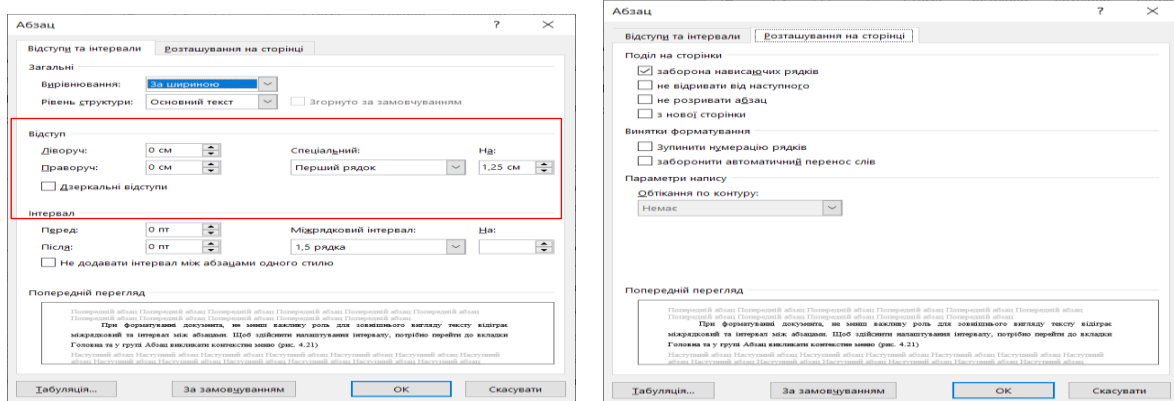


Рис. 20.

Лінійка – інструмент, який використовується для форматування абзаців та дозволяє керувати бічними границями документа і позиціями табуляції.

Границі абзацу (праву, абзацний відступ чи виступ, ліву) задають шляхом переміщення (перетаскування) спеціальних маркерів лінійки. Їх всього чотири. Три ліворуч і один праворуч.



1. Трикутний маркер, розташований ліворуч знизу (вістрям вгору) - задає ліву границю всіх рядків абзаців, крім першого рядка.
2. Перевернений маркер ліворуч зверху (вістрям униз) - задає лінію початку першого рядка.
3. Квадратний маркер під лінійкою . При його перетаскуванні обидва маркери лівої границі переміщуються разом, зі збереженням їхнього відносного

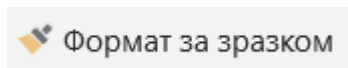
положення.

4. Трикутний маркер праворуч (▲) – задає праву границю всіх рядків абзаців.

При форматуванні документа за допомогою лінійки документ повинний бути представлений у режимі розмітки .

У великих документах більшість абзаців форматується однаково. Якщо бути точним, існує кілька варіантів оформлення абзаців, що багаторазово використовуються в одному документі. Форматувати абзаци у великих документах вручну незручно. Програма WORD вирішує цю проблему, дозволяючи формувати за зразком.

Інструмент **Формат за зразком** (вкладка **Головна** → група **Буфер обміну**



) допомагає скопіювати формат із одного текстового фрагменту та перенести його на інший.

Для того, аби прибрати з фрагмента тексту форматування, доцільно скористатися піктограмою  (вкладка **Головна** → група **Шрифт**), після натискання на яку, формат тексту повернеться до стандартних налаштувань (Шрифт: Calibri (Основний текст), 11 пт; вирівнювання по лівому полю, міжрядковий інтервал: 1,08 (множитель); інтервал між абзацами: 8 пт тощо).

Буквиця, виноска та примітка.

Для створення буквиці (**Б**уквиця – одна велика літера або слово, що складається з великих літер. Створюється з метою візуального виділення абзацу, або художнього оформлення тексту.) у

тексті, необхідно відкрити вкладку **Вставка** та знайти групу **Текст**, у якій знаходиться піктограма  (**Буквиця**). Після натискання на дану піктограму розгортається список, де є доступними два види **Буквиці** на вибір (Рис. 21).

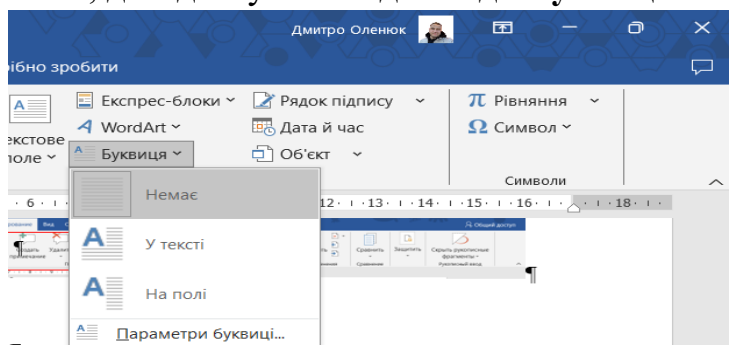


Рис. 21.

Виноска – додатковий пояснювальний текст. Для того, щоб додати у документ виноску, потрібно перейти на вкладку **Посилання** → група **Виноски** (Рис. 22).

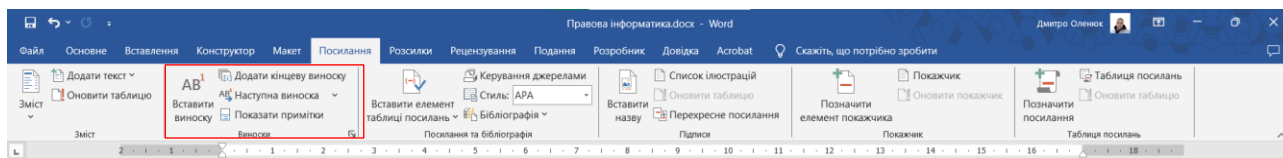


Рис. 22.

Примітки потрібні для того, щоб рецензувати текст, додати коректорські правки та коментарі. Головною особливістю **Приміток**, є те, що вони не відображаються на надрукованому документі. Вставлення приміток у документ відбувається наступним чином: вкладка **Рецензування** → група **Примітки** (Рис. 23). У цій групі відображено інструменти для керування примітками (додавання, видалення, перехід між примітками та їх відображення у документі).

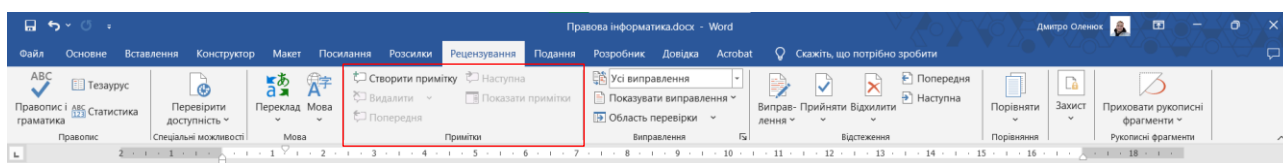


Рис. 23.

Колонки та списки.

Для того, щоб розмістити текст у колонки, потрібно виконати наступні дії:

1. Виділити текст, який необхідно розмістити у вигляді колонок.

Особливістю даної операції є те, що текст потрібно виділяти до останнього надрукованого символу «Кінець абзацу (¶)».

2. Перейти на вкладку **Макет** → група **Параметри сторінки** → **Колонки** та обрати потрібну кількість колонок із списку (Рис. 24).

Якщо користувач потребує більшої кількості колонок, ніж є у списку, тоді потрібно натиснути на

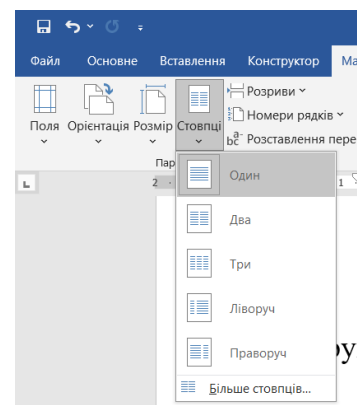


Рис. 24.

Інші колонки (Рис. 25.а) та у діалоговому вікні (Рис. 25.б) здійснити відповідні налаштування.

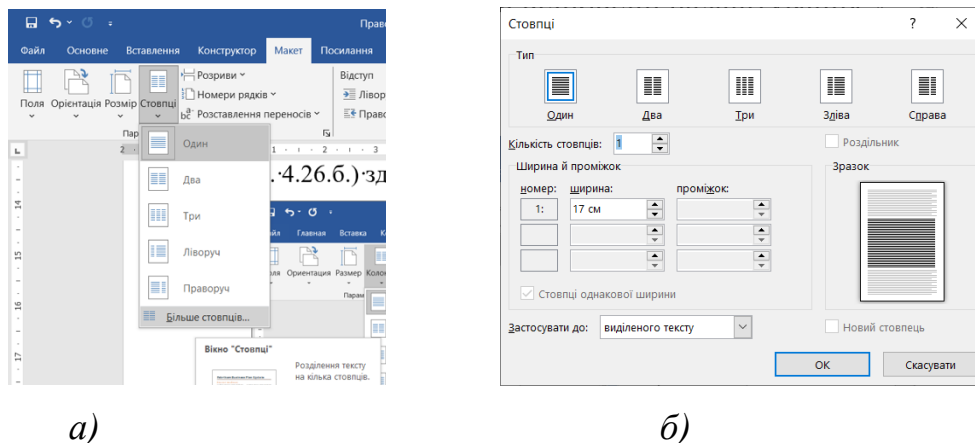


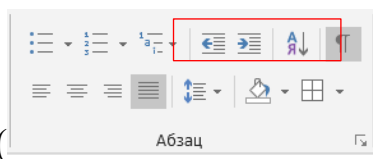
Рис. 25.

У текстових документах розрізняють два основних види списків (нумерований та маркований) і один похідний (багаторівневий). **Нумерований** – це список, кожен пункт якого послідовно нумерується (Рис. 26.а); **маркований** – це список, кожен пункт якого позначається однаковим маркером (Рис. 26.б); **багаторівневий** – це список, який може містити до дев'яти маркованих та/або нумерованих рівнів (Рис. 26.в).



Рис. 26.

Для того, щоб створити список, потрібно перейти на вкладку **Головна** →



група **Абзац** () та обрати потрібний вид списку (маркований – ; нумерований – ; багаторівневий –).

Стилі

Зазвичай текстові документи містять в собі заголовки, підзаголовки, списки та сам текст у вигляді абзаців. Для полегшення роботи, пов'язаної із форматуванням документа використовують **Стилі**. **Стиль** – це набір атрибутів форматування абзаців і символів, якому можна привласнити ім'я.

Можна користуватися вбудованими в WORD стилями, чи створювати свої стилі форматування. Використовуючи вбудований чи створений стиль до обраного тексту, можна легко відформатувати цей текст у відповідності з всіма атрибутами, визначеними в даному стилі. При запуску програми WORD за замовчуванням завантажується і стиль – «Звичайний». Стилі поєднують інформацію про форматування, надану безліччю команд WORD. Група **Стилі** розташована на вкладці **Головна** (Рис. 27).

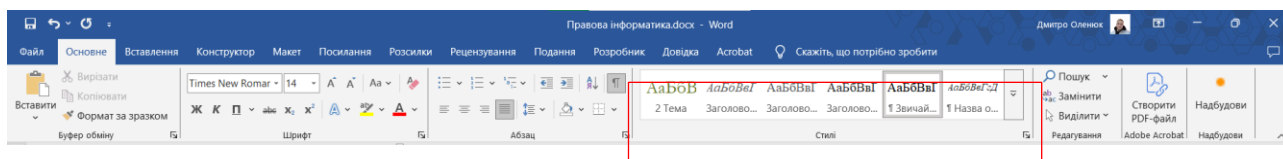


Рис. 27.

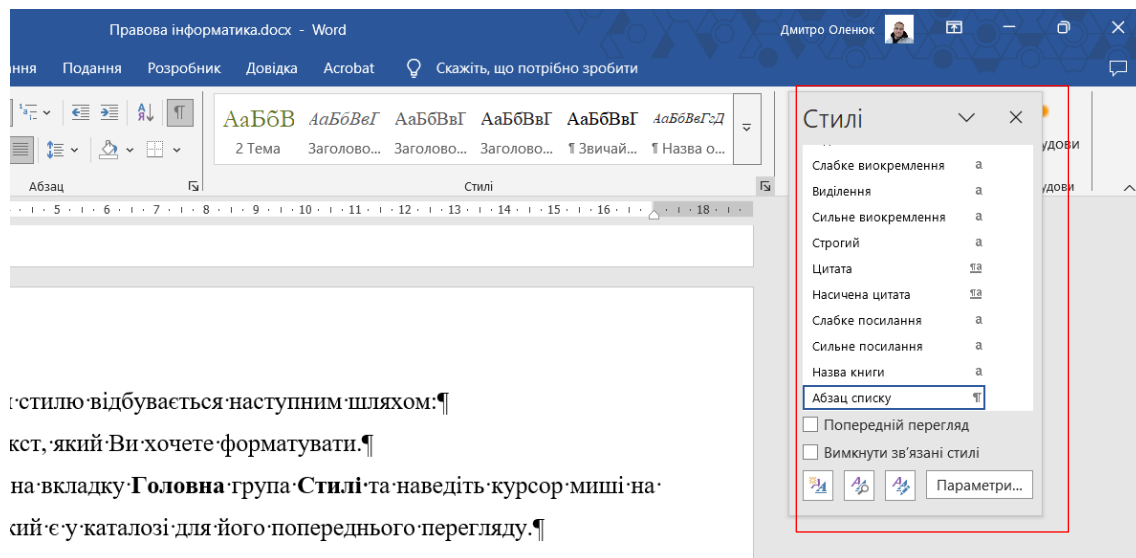
Застосування стилю відбувається наступним шляхом:

1. Оберіть текст, який Ви хочете формувати.
2. Перейдіть на вкладку **Головна** група **Стилі** та наведіть курсор миші на будь-який стиль, який є у каталозі для його попереднього перегляду.
3. Після обрання стилю натисніть на нього лівою кнопкою миші, щоб застосувати.

Запропонований каталог **Стилів** не є вичерпним, і передбачає створення власних стилів із додаванням їх до каталогу, який буде доступний лише у цьому документі або у всіх. Щоб створити власний стиль, потрібно:

1. Перейти на вкладку **Головна** → група **Стилі** та викликати діалогове вікно (Рис. 28). У ньому відображено каталог стилів, піктограми інструментів для роботи зі стилями ( – створити стиль;  – інспектор стилів;  –

керування стилями) і кнопка **Параметри** для керування стилями та самим діалоговим вікном.

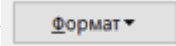


і стилю відбувається наступним шляхом:

кст, який Ви хочете формувати.

на вкладку **Головна** група **Стилі** та наведіть курсор миші на стилі в каталозі для його попереднього перегляду.

Рис. 28.

2. Натиснути на піктограму **Створити стиль** (). Після натискання з'явиться нове діалогове вікно (Рис. 29) у якому можна налаштувати параметри власного стилю із використанням винесених на основну панель інструментів або через меню **Формат** (). Користувач має змогу попередньо переглядати майбутній стиль, який створюється.

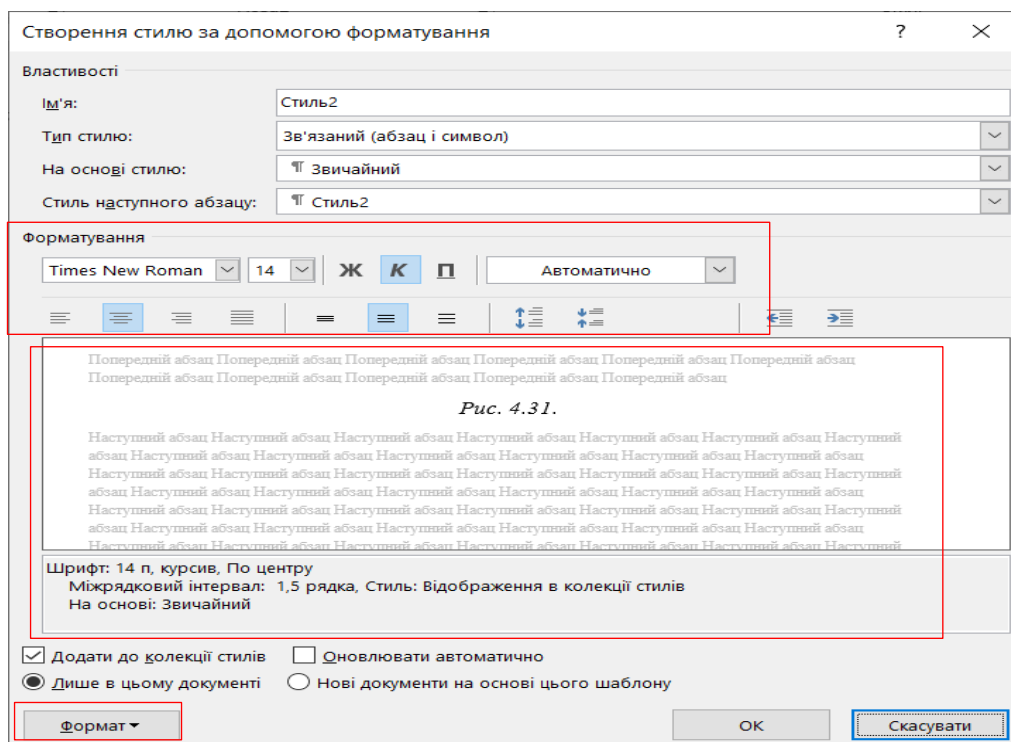


Рис. 29.

Якщо документ не потребує точкового застосування форматування, тоді можна скористатися Конструктором форматування документів. Для цього потрібно перейти на вкладку **Конструктор** → група **Форматування документа** та обрати один із доступних макетів (Рис. 30).

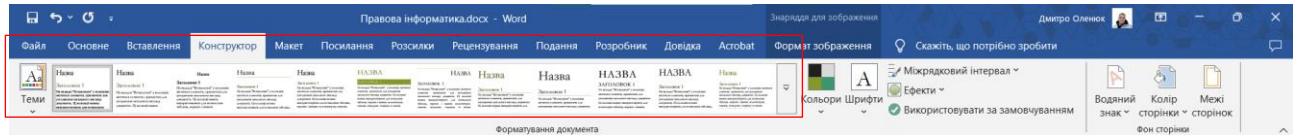


Рис. 30.

Графічні об'єкти.

Програма MS Word містить інструментарій для роботи із графічними об'єктами та в окремих випадках може бути використаний як графічний редактор. WORD має прикладні засоби, що дозволяють вставляти, створювати та формувати графічні об'єкти та математичні формули. Для цих цілей на вкладці **Вставка** розташовано у групі **Ілюстрації** набір інструментів (Рис. 31). Користувач має змогу додати до документу рисунки, які зберігаються у пам'яті ПК або на фізичному носії, зображення з Інтернету, Фігури, SmartArt фігури, діаграми та знімки екрану.

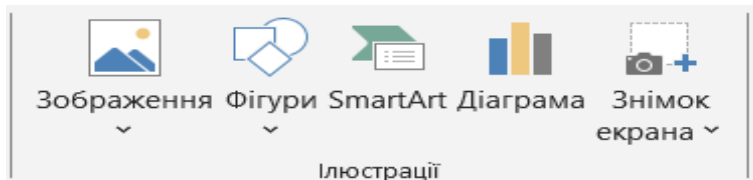


Рис. 31.

Для того, щоб намалювати об'єкт, необхідно клацнути на піктограмі відповідного об'єкта групи **Ілюстрації** збірки **Фігури** (Рис. 32) і за допомогою лівої кнопки миші намалювати його. *Наприклад:* для того щоб намалювати пряму лінію необхідно:

1. Клацнути на піктограмі інструменту лінія .

2. Підвести покажчик в те місце, де повинна починатись лінія.

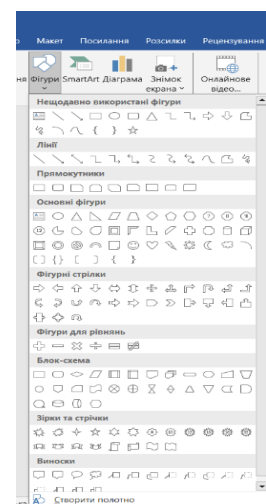


Рис. 32.

3. Натиснути ліву кнопку миші та утримуючи її, перетягнути покажчик миші в місце, де повинен бути кінець лінії.

Використання клавіш при малюванні:

[Shift] – при натисненій клавіші під час малювання лінії будуть горизонтальні чи вертикальні, еліпси та дуги – кругами, а прямокутники – квадратами.

[Ctrl] – при натисненій цієї клавіші об'єкт буде малюватись не від краю, а від центру. [Shift][Ctrl] – об'єкти малюються правильної форми і від центру.

У Microsoft Word ви можете створювати графічні об'єкти з використанням полотна, яке дозволяє вам вільно розташовувати, малювати та оформлювати графічні елементи.

Таблиці.

У Microsoft Word таблиці використовуються для організації, представлення та форматування даних у вигляді сітки з рядками і стовпцями. Вони надають зручний спосіб візуального представлення і структурування інформації. Таблиці у Microsoft Word (Рис. 33.) є потужним інструментом для структурування та оформлення даних в документах. Вони можуть бути використані для розташування числових даних, тексту, зображень або комбінації цих елементів. Створення таблиць у Word дозволяє вам організувати інформацію в зручний спосіб, забезпечуючи чіткість та доступність даних.

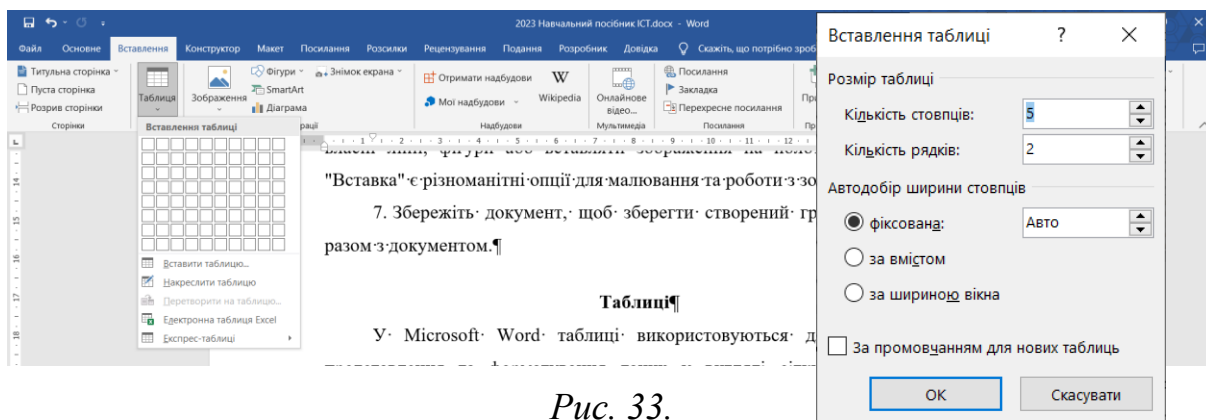


Рис. 33.

Для створення таблиці в Word ви можете скористатися різними методами. Найпростіший спосіб – використання команди **Вставити** таблицю на вкладці

Вставка. Виберіть кількість рядків та стовпців, а Word автоматично створить пусту таблицю для вас. Ви також можете малювати таблицю, визначаючи контур її клітин. Після створення таблиці ви можете заповнити її даними. Вставляйте текст, числа, зображення або комбінації цих елементів у відповідні клітинки. Ви можете формувати текст, застосовувати кольори, шрифти, стилі або надавати коміркам і рамкам різні вигляди за допомогою опцій форматування, доступних на вкладці **Таблиці** інструментів.

Однією з функцій таблиць у Word є можливість виконувати розрахунки за допомогою формул. Ви можете додавати, віднімати, множити або ділити значення в комірках, використовуючи вбудовані функції або створюючи власні формули. Це дозволяє вам автоматизувати обчислення та аналіз даних у таблицях.

Діаграми у Word – це інструмент для візуалізації та презентації даних. Завдяки різноманіттю доступних діаграм та інструментів редагування, ви можете створити оригінальні та професійні графіки, що допоможуть зрозуміти та показати важливу інформацію (Рис. 34.).

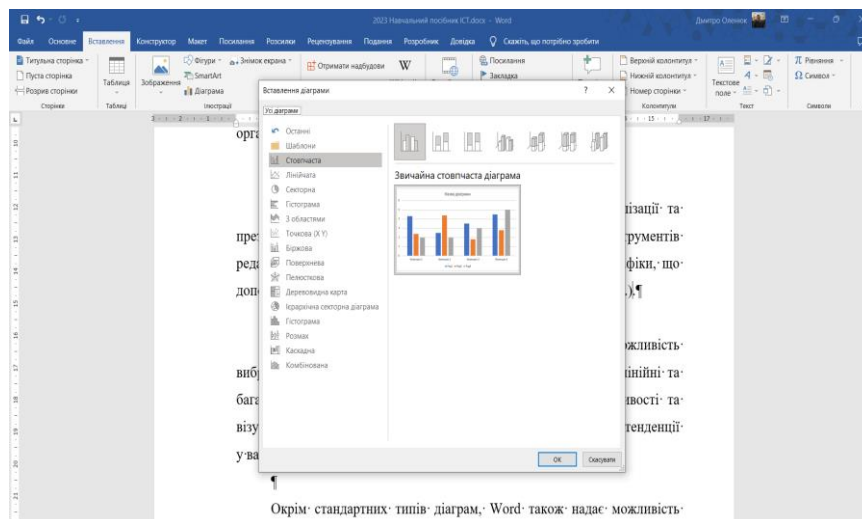


Рис. 34.

Коли ви працюєте з діаграмами у Word, вам надається можливість вибрати з різних типів діаграм, таких як стовпчасті, кругові, лінійні та багато інших. Кожен тип діаграми має свої унікальні можливості та візуальні ефекти, які дозволяють вам підкреслити основні точки та тенденції у ваших даних.

Окрім стандартних типів діаграм, Word також надає можливість налаштування вигляду діаграми, змінюючи кольори, шрифти, фон та інші параметри. Це дозволяє створити оригінальний дизайн діаграми, який відповідає вашому стилю та потребам.

Крім того, Word надає розширені можливості редагування діаграм, що дозволяють додавати та формувати текстові елементи, легенду, мітки даних та інше. Можна використовувати ці функції для підкреслення ключової інформації або пояснення важливих аспектів даних, представлених на діаграмі. Загалом, діаграми у Word дозволяють створити оригінальні та професійні графіки, що допоможуть ефективно візуалізувати інформацію.

Шаблони у Word – це передвстановлені форматування та макети, які дозволяють швидко створювати професійно виглядаючі документи. Вони включають заздалегідь налаштовані стилі, шрифти, колірні схеми та розміщення елементів сторінки, що дозволяє економити час та зусилля при створенні нових документів. Word надає великий вибір шаблонів для різних типів документів, таких як резюме, листи, звіти, презентації, брошури та багато інших. Кожен шаблон має свою унікальну структуру та дизайн, відповідаючи вимогам і стандартам кожного типу документа.

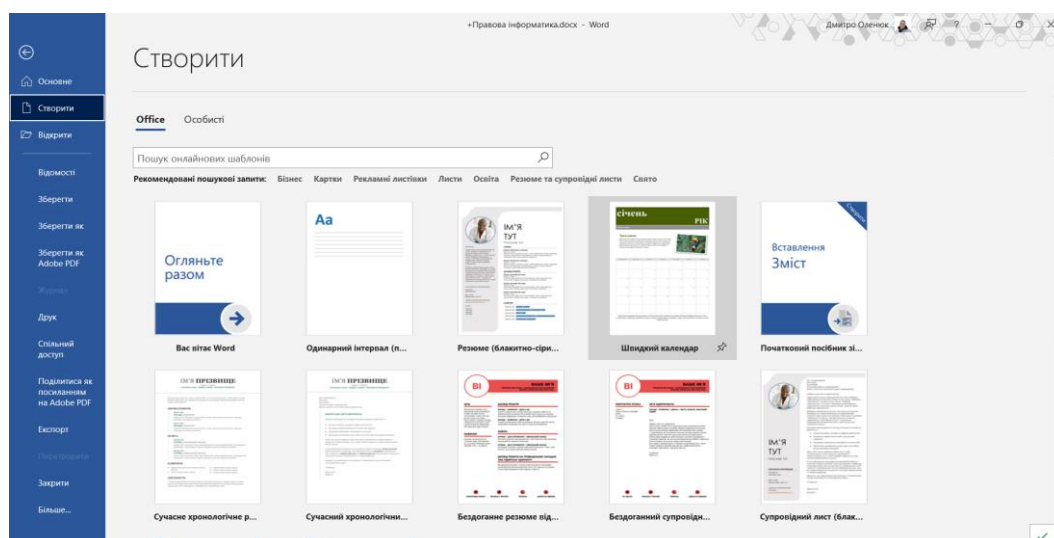


Рис. 35.

За допомогою шаблонів, можна швидко розпочати роботу над документом, вибравши відповідний шаблон та заповнивши його власним вмістом. Можна налаштувати шаблон, додавши або видаливши розділи, таблиці, зображення,

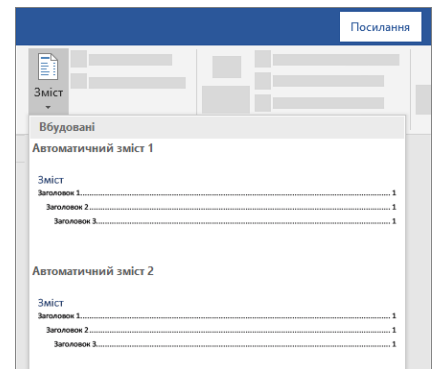
графіки або інші елементи, щоб він відповідав вашим потребам та стилю. Однією з переваг використання шаблонів у Word є їх гнучкість та настроювання. Адже можна змінювати кольори, шрифти, макети та інші параметри шаблону, а також зберігати власні налаштування як новий шаблон для майбутнього використання.

Використання шаблонів у Word полегшує процес створення документів, забезпечуючи професійний вигляд і зберігаючи послідовність форматування.

Робота з великими документами.

При роботі з великими документами в Word, створення змісту, списку ілюстрацій та предметного покажчика є важливими елементами, які допомагають зручно навігувати і знайти необхідну інформацію в документі. Ці функції дозволяють організувати й індексувати вміст вашого документа, забезпечуючи зручний доступ до його різних частин.

Зміст документа – це перелік розділів, підрозділів та інших елементів, які входять до вашого документа, разом з номерами сторінок, на яких вони розташовані. У Word ви можете автоматично створити зміст, використовуючи стилі заголовків і вбудовані інструменти. Застосуйте стилі до розділів та підрозділів, а потім вставте зміст, щоб створити автоматично оновлюваний перелік.



Список ілюстрацій включає всі зображення, схеми, таблиці або інші графічні елементи, що містяться в документі, разом з їх підписами та номерами сторінок. Ви можете створити список ілюстрацій у Word, використовуючи вбудований інструмент Підписи. Додайте підписи до своїх ілюстрацій та вставте список, щоб автоматично зібрати всі ілюстрації разом з їх номерами сторінок. *Предметний покажчик* – це алфавітний перелік ключових термінів або термінів, використаних у вашому документі, разом з номерами сторінок, на яких вони зустрічаються. Щоб створити предметний покажчик у Word, можна використовувати функцію Покажчик або Огляд і додавати відповідні записи до списку термінів та сторінок.

Довідка MS Word. Користувач, у якого виникають запитання стосовно роботи із текстовим процесором може скористатися **Довідкою**. Для цього потрібно

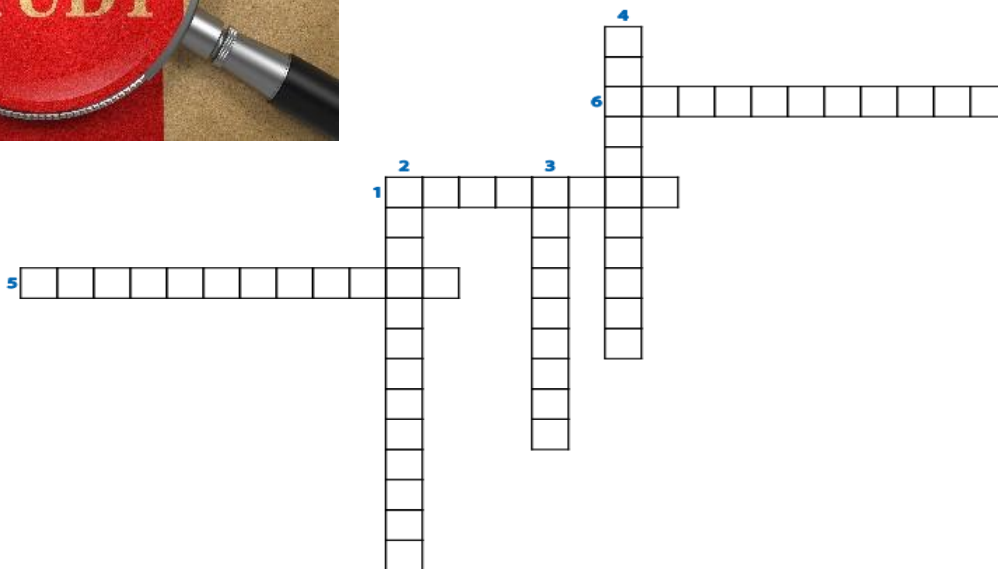
натиснути на клавішу **F1**, яка викликає діалогове вікно, що складається із пошукової стрічки та каталогу категорій. Також, користувачі можуть скористатися безкоштовним онлайн-сервісом «**Центр довідки та навчання Office**»¹⁶⁰ для отримання інформації по роботі з офісними застосунками від Microsoft.

Варто відзначити, що навички автоматизації юридичних документів, зокрема використання шаблонів, макросів, функцій автозаповнення та створення інтегрованих схем і діаграм, є невід'ємною складовою цифрової компетентності сучасного юриста. Опанування відповідних навичок є особливо важливим для практикуючих юристів, оскільки в умовах сучасної юридичної діяльності часто виникає потреба не лише якісно оформити правові документи, а й створювати зрозумілі схеми, діаграми, графічні візуалізації процесів і структур, що підвищує ефективність комунікації з клієнтами та колегами.



ПЕРЕВІРКА ЗНАНЬ

Для закріплення пройденого матеріалу розв'яжіть кросворд.



По горизонталі: 1. Protection of legal information from leaks and manipulations.. 5. Openness of legal information to citizens (except for confidential data).. 6. The property of legal information that depends on its conformity to the actual state of affairs..

По вертикалі: 2. Clear hierarchy and logical connections between sources of law.. 3. The need for regular updates of legal information due to changes in legislation.. 4. The official nature of legal information, backed by state enforcement..

¹⁶⁰ Microsoft. Підтримка Word. URL: <https://support.microsoft.com/uk-ua/word> (дата звернення: 29 квітня 2025 р.).

ЗАВДАННЯ

**1. Debate «Can cloud technologies completely replace paper document flow in the legal field?»**

Підготуйте аргументи за та проти використання хмарних технологій для повного переходу на електронний документообіг у юридичній практиці. Обговоріть питання безпеки, конфіденційності та правового регулювання.

**2. Discussion «Problems of information security in Ukraine under modern conditions»**

Сформулюйте пропозиції щодо поліпшення законодавчого регулювання питань інформаційної та кібербезпеки в сучасних умовах. Додайте приклади з реальними кейсами, щодо питань інформаційної та кібербезпеки, які вам відомі.

**3. Teamwork «Creating Infographics»**

На основі запропонованої тематики створіть інфографіку з використанням доступних для вас онлайн-сервісів.

- *Інфографіка про вимоги GDPR та Закону України «Про захист персональних даних».*
- *Моделі хмарних послуг (IaaS, PaaS, SaaS) та їх використання в юридичній практиці.*
- *Вимоги до електронних документів згідно із законодавством.*

**4. Construct a diagram**

Побудуйте діаграму, що ілюструє статистичні показники народжуваності та смертності в Україні у період з 2021 по 2024 рік.

Статистична інформація міститься на офіційному вебсайті [Міністерства юстиції України](https://minjust.gov.ua/actual-info/stat_info)¹⁶¹.



5. Create your own CV (Curriculum Vitae)

Скористайтесь шаблонами текстового процесора Word для укладення власного резюме відповідно до вимог сучасного ділового стилю. Не забудьте використовувати де потрібно нерозривні пропуски.

¹⁶¹ Офіційний вебсайт Міністерства юстиції України. Статистична інформація щодо державної реєстрації актів цивільного стану. URL: https://minjust.gov.ua/actual-info/stat_info (дата звернення: 29.04.2025)

Розділ XI ЕЛЕКТРОННИЙ СУД

E-COURT

1. Досвід України



Сьогодні, кожна сфера суспільного життя в Україні, зокрема: охорона здоров'я, громадський порядок та безпека, освіта, культура та ін., зазнала процесів цифровізації. Це обумовлено рядом причин, а саме: стрімким розвитком інформаційних технологій завдяки яким є можливість оптимізувати та значно спростити певні процеси; суспільною необхідністю, яка полягає у створенні доступних умов для отримання відповідних послуг громадян; оперативністю в отриманні бажаних результатів та економічністю, оскільки наразі, не потрібно особисто прибувати, до прикладу, в центр надання адміністративних послуг для декларування місця реєстрації, адже це можливо зробити через застосунок «Дія». Застосунок «Дія» – це яскравий приклад взаємодії держави і громадянина, яка полягає у вирішенні ряду питань та проблем, не виходячи з власного помешкання.

Однак, трапляються різні життєві ситуації, коли порушуються права та законні інтереси людини, і для того щоб їх відновити потрібно звернутися до суду. В Україні діє чітка ієрархічна система судів, які спеціалізуються на розгляді кримінальних, цивільних, адміністративних та господарських справ.

Для того, щоб звернутися до суду, до 2018 року, потрібно було підготувати позивачу позовну заяву та надіслати поштовою кореспонденцією на адресу або ж особисто занести в канцелярію суду.

Підвідомчість судових справ є різна, наприклад у господарських спорах, майно відповідача – боржника може знаходитися у Миколаївській області (де і

буде розглядатися справа), а позивач у Житомирській області. Отже було два варіанти для позивача: надіслати позовну заяву поштою або ж особисто відвідати відповідний суд, це стосується і подальшої участі у судових засіданнях. В результаті для позивача виникають проблеми, які пов'язані з транспортуванням, затратою часу та коштів.

Усвідомлюючи необхідність осучаснити можливість особи звернутися до суду, з 4 червня 2018 було введено в тестову експлуатацію підсистему ЄСІТС «Електронний суд», до якої початково доєднані 18 пілотних судів. У номері «Голосу України» за 1 грудня 2018 опубліковано оголошення про створення та забезпечення функціонування Єдиної судової інформаційно-телекомунікаційної системи¹⁶².

Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) – сукупність інформаційних та телекомунікаційних підсистем (модулів), які забезпечують автоматизацію визначених законодавством та Положенням про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи процесів діяльності судів, органів та установ в системі правосуддя, включаючи документообіг, автоматизований розподіл справ, обмін документами між судом та учасниками судового процесу, фіксування судового процесу та участь учасників судового процесу у судовому засіданні в режимі відеоконференції, складання оперативної та аналітичної звітності, надання інформаційної допомоги суддям, а також автоматизацію процесів, які забезпечують фінансові, майнові, організаційні, кадрові, інформаційно-телекомунікаційні та інші потреби користувачів ЄСІТС. Починаючи з 05.10.2021 функціонують три підсистеми (модулі) ЄСІТС - «Електронний кабінет», «Електронний суд» та підсистема відеоконференцзв'язку¹⁶³.

¹⁶² ДСА України оголосила про створення та функціонування Єдиної судової інформаційно-телекомунікаційної системи. *Державна судова адміністрація України*. URL: <https://web.archive.org/web/20201001202958/https://court.gov.ua/press/news/611254/> (дата звернення: 31.03.2025).

¹⁶³ Функціонування Єдиної судової інформаційно-комунікаційної системи. *Державна судова адміністрація України*. URL: https://dsa.court.gov.ua/dsa/inshe/func_ecits/ (дата звернення: 31.03.2025).

«Електронний суд» забезпечує обмін процесуальними документами (надсилання та отримання документів) в електронній формі між судами, органами та установами системи правосуддя, між судом та учасниками судового процесу, між самими учасниками судового процесу. Він дає оперативність та зручність у комунікації суду із сторонами у справах¹⁶⁴.



```
graph TD; A[ЯК ПОЧАТИ КОРИСТУВАТИСЯ ПІДСИСТЕМОЮ «ЕЛЕКТРОННИЙ СУД»?] --> B[ПЕРЕЙТИ НА САЙТ  
HTTPS://ID.COURT.GOV.UA/]; B --> C[ЗАЙСНИТИ РЕЕСТРАЦІЮ ОФІЦІЙНОЇ ЕЛЕКТРОННОЇ АДРЕСИ  
(ЕЛЕКТРОННОГО КАБІНЕТУ)]; C --> D[РЕЕСТРАЦІЯ ТА ПОДАВАННЯ АВТЕНТИФІКАЦІЇ  
КОРИСТУВАЧІВ ЗАЙСНИЄТЬСЯ ЗА ДОПОМОГОЮ  
ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДСИСУ  
(ЕЛЕКТРОННИЙ КЛЮЧ) КОРИСТУВАЧА];
```

ЕЛЕКТРОННИЙ СУД

ЕЛЕКТРОННИЙ СУД
court.gov.ua / ecourt.gov.ua

ЯК ПОЧАТИ КОРИСТУВАТИСЯ ПІДСИСТЕМОЮ «ЕЛЕКТРОННИЙ СУД»?

ПЕРЕЙТИ НА САЙТ
[HTTPS://ID.COURT.GOV.UA/](https://id.court.gov.ua/)

ЗАЙСНИТИ РЕЕСТРАЦІЮ ОФІЦІЙНОЇ ЕЛЕКТРОННОЇ АДРЕСИ
(ЕЛЕКТРОННОГО КАБІНЕТУ)

РЕЕСТРАЦІЯ ТА ПОДАВАННЯ АВТЕНТИФІКАЦІЇ
КОРИСТУВАЧІВ ЗАЙСНИЄТЬСЯ ЗА ДОПОМОГОЮ
ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДСИСУ
(ЕЛЕКТРОННИЙ КЛЮЧ) КОРИСТУВАЧА



¹⁶⁶ Покрокова інструкція з реєстрації в «Електронному суді». *Державна судово адміністрація України*. URL: <https://zp.arbitr.gov.ua/sud5009/gromadyanam/el-sud-reg/> (дата звернення: 31.03.2025).

ПРОЦЕДУРА РЕЄСТРАЦІЇ

КРОК 2. ПЕРЕВІРТЕ ДАНІ, ЯКІ ВІДОБРАЗАЮТЬСЯ АВТОМАТИЧНО І ВВЕДІТЬ ТІ, ЯКИХ НЕ ВИСТАЧАЄ

Електронний Суд
Офіційна електронна адреса: court.gov.ua/e-court/

Для завершення реєстрації заповніть наступні дані:

Прізвище
Ім'я
По батькові
Дата народження
Унікальний номер облікового запису (Ідентифікаційний номер громадянина України (ID))
☐ Я є особою-фізичною
Номер телефону
Електронна адреса
☐ Я є представником з укладання користувачем судових актів електронного кабінету

Підтвердити

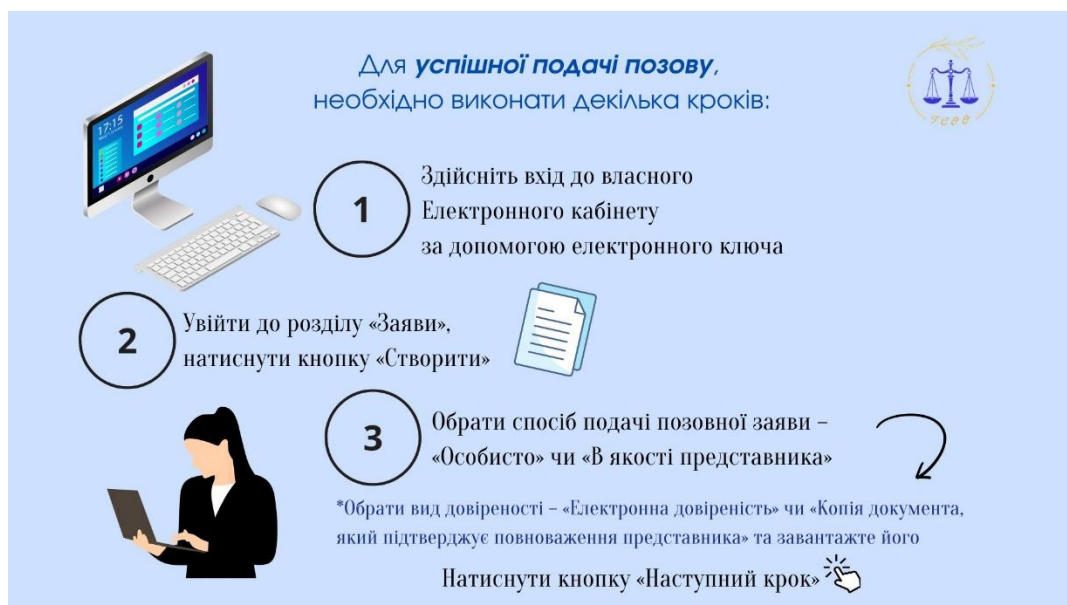
ВІТАЄМО! ВИ СТАЛИ ПОВНОЦІННИМ КОРИСТУВАЧЕМ ПІДСИСТЕМИ «ЕЛЕКТРОННИЙ СУД».

Електронний Суд
Офіційна електронна адреса: court.gov.ua/e-court/

Повідомлень немає
Тут будуть відображатися всі повідомлення про зміни статусів справ, відкриття справ, отримання довіреностей тощо.

Вхід
Мої справи
Заяви
Дізнання
Справи
Статистика
Екран

Як подати позовну заяву через підсистему «Електронний суд»¹⁶⁷ ?



¹⁶⁷ Подання позовної заяви через підсистему "Електронний суд": покрокова інструкція від Господарського суду Одеської області. Державна судова адміністрація України. URL: <https://court.gov.ua/press/news/1647311/> (дата звернення: 31.03.2025).

4

Обрати форму заяви із запропонованого переліку, потім зазначити вид судочинства, категорію та підкатегорію справи або ввести назву заяви в полі для пошуку шаблону



5

Заповнити наступні розділи:

- регіон та суд;
- позивач;
- представник позивача;
- відповідач (юридична або фізична особа);
- інші учасники;
- ціна позову.



6

Заповніть розділ "текст заяви", якщо потрібно – ознайомтесь із прикладом, натиснувши на посилання



7

Підтвердження (підтвердити, що позивачем не подано іншого позову/позовів до цього ж відповідача/відповідачів з тим самим предметом та з тих самих підстав поставивши «V»)



8

Завантажте додатки та натисніть кнопку "Зберегти", після чого – обов'язково задайте назву цим документам і натисніть "Підтвердити" ✓



9

На цьому етапі необхідно уважно розрахувати та сплатити судовий збір.



У РАЗІ, ЯКЩО ВИ ЗАЗДАЛЕГІДЬ СПЛАТИЛИ СУДОВИЙ ЗБІР, необхідно завантажити квитанцію у розділ "Додатки"

Для цього поставте відмітку у полі «Я звільнений(-а) від сплати судового збору згідно ст. 5 ЗУ «Про судовий збір» або збір вже сплачено»



9.1

Оберіть зі списку «Судовий збір сплачено» та завантажте квитанцію про сплату.



9.2

ЯКЩО ПОЗИВАЧ ЗВІЛЬНЕНИЙ
ВІД СПЛАТИ СУДОВОГО ЗБОРУ
ЗГІДНО СТ. 5 ЗУ «ПРО СУДОВИЙ ЗБІР»





- Поставте відмітку у полі «Я звільнений(-а) від сплати судового збору згідно ст. 5 ЗУ «Про судовий збір» або збір вже сплачено».
- У графі «Пільги» оберіть категорію, до якої Ви належите.
- Прикріпіть електронну копію підтверджуючого документа за допомогою кнопки «Завантажити документ».

10 Натисніть кнопку «Сформувати заяву», після чого, підпишіть її за допомогою КЕП (кваліфікованого електронного підпису)



11 Наступним важливим кроком є **НАДІСЛАННЯ КОПІЙ ЗАЯВИ СТОРОНАМ**. У відповідній графі позначте сторін, яким необхідно надіслати копію документа. Відповідна квитанція буде автоматично завантажена до додатків. Потім натисніть кнопку "Підписати та відправити"




12 Сформувати квитанцію про доставку документів до зареєстрованого Електронного кабінету Користувача ЄСІТС




Іншим важливим моментом, на який варто звернути увагу, є те, що новими процесуальними кодексами передбачено, що суд проводить розгляд справи за матеріалами судової справи в електронній формі. У такому разі всі процесуальні та інші документи переводяться в електронну форму та долучаються до матеріалів електронної судової справи. Безумовно, такі нововведення є вкрай позитивними, адже електронне судочинство значною мірою підвищує ефективність правосуддя в цілому, спрощує доступ до справи її учасників, а також заощаджує організаційні, фінансові та часові затрати, пов'язані з

пересиланням матеріалів справи з одного суду до іншого та ознайомленням з ними учасників¹⁶⁸.

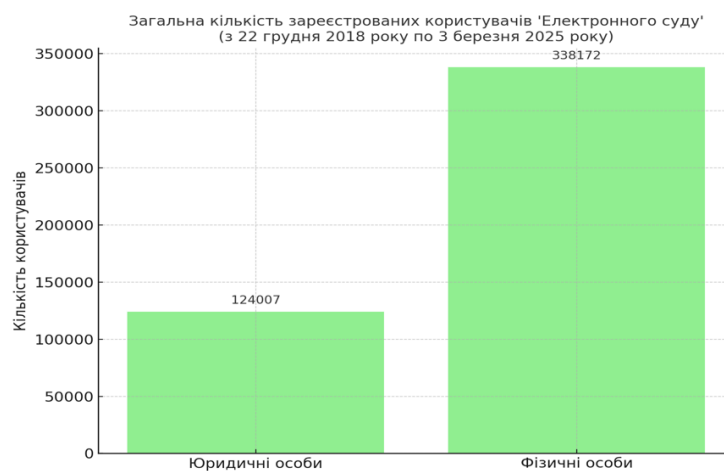
Звісно, під час експлуатації трапляються технічні проблеми, спричинені різними обставинами, в тому числі хакерськими атаками. Однак, фахівці Державного підприємства «Інформаційні судові системи» намагаються оперативно усунути інформаційні загрози та нормалізувати роботу ЄСІТС.

Як свідчать дані ДП «ІСС», кількість користувачів підсистеми ЄСІТС «Електронний суд» зростає щодня на 420 осіб¹⁶⁹.

З 1 січня 2025 року по 03 березня 2025 року кількість зареєстрованих користувачів «Електронного суду» зросла на 26 065 осіб.



З початку впровадження системи 22 грудня 2018 року загальна кількість зареєстрованих користувачів «Електронного суду» досягла 454 678 осіб, з яких:



¹⁶⁸ Пономаренко В. «Електронний суд»: недоліки та переваги. URL: <https://ndipzir.org.ua/wp-content/uploads/2019/26.02.19/26.02.19-53-55.pdf> (дата звернення: 31.03.2025).

¹⁶⁹ Кількість користувачів підсистеми ЄСІТС «Електронний суд» зростає щодня на 420 осіб. Судова влада України. URL: <https://ics.gov.ua/ics/news/novyny/1766855/> (дата звернення: 31.03.2025).

Зросла і кількість заяв, які користувачі «Електронного суду» подають через «Електронний кабінет». Так, з 1 січня 2025 року було надіслано 682 628 заяв через сервіс «Електронний кабінет», а з часу впровадження системи (22 грудня 2018 року) надіслано за допомогою сервісу «Електронний суд» 6 086 733 заяви.

Зазначені цифри є підтвердженням зручності та популярності використання підсистеми «Електронний суд».

Можливо у недалекому майбутньому, у всіх судах справи судді розглядатимуть лише у електронній формі та сотні тисяч дерев будуть збережені.



З практичного досвіду. Певні суди України тестували розгляд справ у електронній формі. За підсумками зроблено наступні висновки, це дозволяє:

- дотримуватись принципу процесуальної економії, адже забезпечує можливість оперативного обміну електронними документами між судом та учасниками судового процесу;
- швидко отримувати учасниками судової справи інформації про рух справи, а також процесуальні документи за наслідками розгляду справи, що зменшує тривалість розгляду судових справ у суді;
- суттєво економити кошти державного бюджету на закупівлі офісного паперу, заправці картриджів для принтерів, а також витратах на пересилання поштової кореспонденції;
- створити більше умов для забезпечення прозорості діяльності судів та підвищення рівня довіри до суду, як органу правосуддя, тощо¹⁷⁰.

Не виключено запровадження штучного інтелекту для розгляду судових справ в Україні. Це інноваційне рішення активно тестується в інших країнах.

¹⁷⁰ Курілов Є. Восьмий апеляційний адміністративний суд вперше розглянув справу виключно в електронній формі. URL: <https://azones.law/news/vosmyj-apelyatsijnyj-administrativnyj-sud-vpershe-rozglyanuv-spravu-vyklyuchno-v-elektronnij-formi/> (дата звернення: 31.03.2025).

2. Іноземний досвід



У Китаї штучний інтелект повністю інтегрували у правову систему. Про це повідомляє видання South China Morning Post¹⁷¹. Згідно зі звітом Верховного народного суду КНР, штучний інтелект типу система систем (smart court SoS system of systems) тепер підключений до комп'ютера кожного судді на території Китаю. Програма автоматично пропонує номери схожих судових справ, а також рекомендує закони та ухвали. Крім того, штучний інтелект складає проекти юридичних документів та виправляє передбачувані людські помилки у вироку. Також штучний інтелект скоротив середнє робоче навантаження суддів більш ніж на третину. З 2019 до 2021 року програма заощадила громадянам Китаю 1,7 млрд робочих годин.



У Німеччині, наприклад, в складних справах у судовому доказуванні використовують VR-технології. Першим прикладом такого використання була справа колишнього наглядача концтабору Райнхольда Ганнінга, яка розглядалася судом Детмольда у 2016 році. Ганнінг звинувачувався у вбивстві 170 000 осіб, однак стверджував, що виконував лише охоронну службу і не міг бачити, що відбувалося в таборі. Тому слідчі за допомогою лазерного сканера розробили VR-модель табору на основі фотографій та будівельних планів. Вони змогли віртуально розташуватись на вежі охорони і довести, що Ганнінг мав пряму лінію огляду як табору так і місця «фільтрації» депортованих людей.

Наступним цікавим випадком використання VR-технологій під час доказування є «справа гонщика з Вісбадена». 25-річний хлопець мчав по місту на авто зі швидкістю 130 км/год і спричинив аварію, внаслідок якої на наступний день від численних травм загинув 30-річний батько родини. При огляді місця

¹⁷¹ У Китаї штучний інтелект повністю інтегрували у правову систему. Судово-юридична газета. URL: <https://sud.ua/uk/news/abroad/244322-v-kitae-iskusstvennyy-intellekt-polnostyu-integrirovali-v-pravovuyu-sistemu> (дата звернення: 31.03.2025).

події на транспортних засобах обвинуваченого та жертви були встановлені на рівні очей 360-градусні камери. Це дало змогу пізніше додатково оцінити видимість учасників ДТП у момент аварії, адже найсуворіша санкція інкримінованого злочину за німецьким кримінальним кодексом передбачає довічне ув'язнення. До чого й було пізніше засуджено молодого водія¹⁷².



Суддя із Флориди у 2024 році був першим в Америці, хто також



використав 3D-окуляри під час судового розгляду для огляду місця злочину¹⁷³. Хоча інноваційний вид доказування є дуже захоплюючим та потужним, однак він несе із собою також й унікальні проблеми, адже з пасивного слухача, учасник судового процесу за допомогою VR-технологій перетворюється на задіяну у злочині особу, що в сукупності впливає на сприйняття обставин, емоції та пам'ять. Так, наприклад, у розглядуваній справі саме захист використав VR для реконструкції подій, однак це призвело до звинувачень у нападі за обтяжливими обставинами¹⁷⁴.



Втім, у Колумбії ще у лютому 2023 року було проведене перше у світі двогодинне судове засідання повністю у метавсесвіті¹⁷⁵.



¹⁷²Костенко С. VR-технології як новий вимір доказування: виклики для країни та юридичної освіти DOI 10.36074/logos-07.03.2025.022

¹⁷³ Judge dons VR headset in what's thought to be courtroom first. URL: <https://www.youtube.com/watch?v=JXSGWSSZ80A> (date of access 31.03.2025).

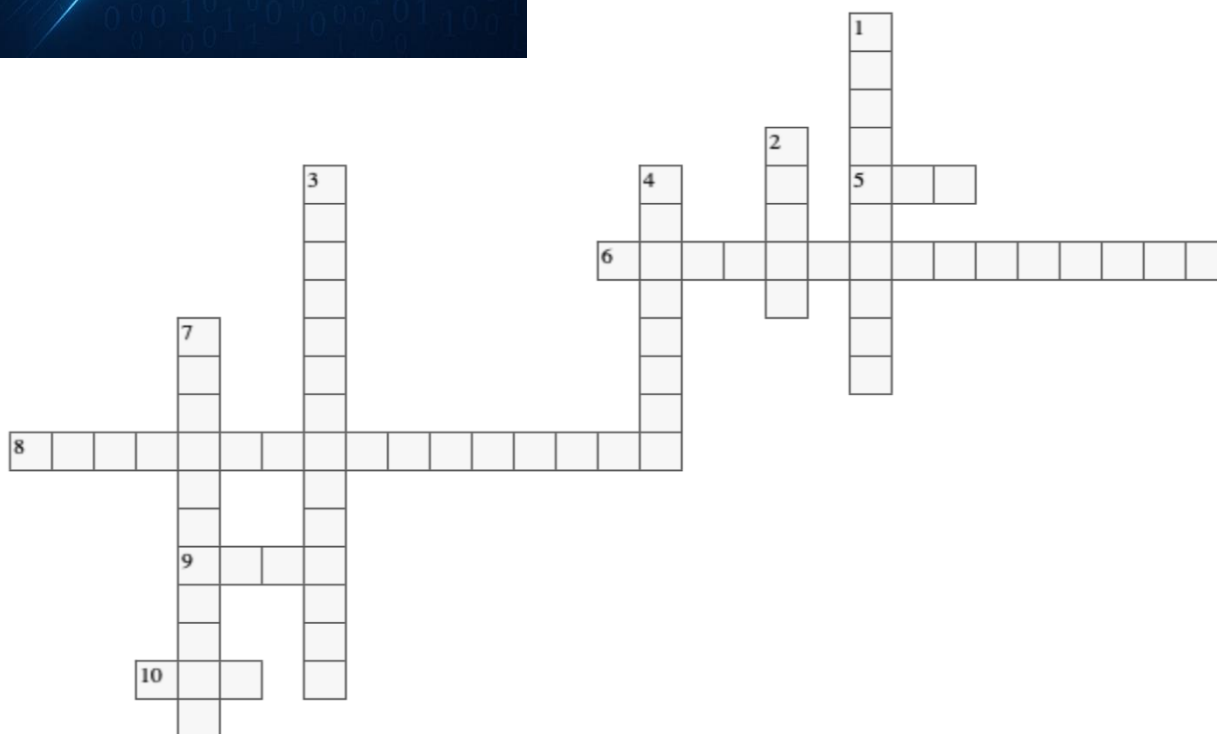
¹⁷⁴ Schlegel S. From Foam Board to Virtual Reality: A Judge's Perspective on the Latest Evolution in Demonstrative Evidence. Legal Tech, 2025. URL: https://judgeschlegel.substack.com/p/from-foam-board-to-virtual-reality?utm_campaign=post&utm_medium=web (date of access 31.03.2025).

¹⁷⁵ Colombian court holds 2-3 hour long virtual court hearing. WION. URL: <https://www.youtube.com/watch?v=JuFIVMPF004> (date of access 31.03.2025).



ПЕРЕВІРКА ЗНАНЬ

Для закріплення пройденого матеріалу розв'яжіть кросворд. Деякі відповіді складаються з двох слів – вони записуються без пробілу.



По горизонталі

5. Скільки модулів Єдиної судової системи запроваджено в Україні?
6. За допомогою чого здійснюється автентифікація користувача?
8. Одна з головних переваг електронного суду — можливість брати участь у засіданні у цьому режимі.
9. Технічна перешкода, яка може завадити роботі електронного суду.
10. Через який застосунок можна задекларувати місце проживання без відвідування ЦНАП?

По вертикалі

1. Яка форма розгляду судових справ передбачена новими процесуальними кодексами України?
2. Скорочена назва єдиної судової системи, яка автоматизує роботу судів.
3. Як називається підсистема, що дозволяє подавати документи до суду онлайн?
4. У якій країні відбулося перше судове засідання у метавсесвіті?
7. Дія, яку виконує користувач для входу в систему електронного суду?

ЗАВДАННЯ

**1. Comparative Analysis: Traditional vs Electronic Justice**

Порівняйте переваги та недоліки традиційного і електронного судочинства. Підготуйте презентацію або есе на тему: *«Чи замінить електронний суд традиційні форми правосуддя?»*.

**2. Legal Case Analysis**

Ситуація: через технічний збій у системі «Електронний суд» ваш клієнт не зміг подати апеляцію вчасно.

Якими мають бути подальші дії? Підготуйте необхідні процесуальні документи.

**3. Practical Case**

Складіть позовну заяву або інший процесуальний документ (наприклад, апеляційну скаргу) відповідно до вимог електронного судочинства. Зверніть увагу на форматування, електронний підпис і вимоги до подання документів через систему. Випишіть додаткові вимоги до електронного судочинства та представте їх на занятті.

Розділ XII «РОЗУМНЕ» МІСТО SMART CITY

1. Походження та становлення концепції „Smart City“

Концепція «Smart City» сформувалася відносно нещодавно, наприкінці XX – на початку XXI століття. На початку в її основі лежали ідеї, що поєднували міський розвиток з новітніми технологіями. Так, ще у 1980-х роках з'явилися поняття «intelligent city» («інтелектуальне місто») та «digital city» («цифрове місто»), які виражали ранні спроби показати взаємозв'язок в процесах використання обчислювальної техніки і телекомунікацій з функціонуванням та розвитком міст¹⁷⁶. Однак тоді ці ідеї носили швидше футуристичний або навіть експериментальний характер.



Першим містом, в якому такий «експеримент» знайшов своє безпосереднє втілення прийнято вважати Амстердам (Нідерланди), де у 1994 р. було створено віртуальне «цифрове місто» De Digitale Stad (DDS), як онлайн-платформу для взаємодії його мешканців. Цей проєкт сприяв розвитку електронної демократії та громадської участі через інтернет, що є ключовими аспектами концепції «розумного міста»¹⁷⁷.

Слід зазначити, що в публікаціях академічного характеру фактично до 1990-х років поняття «Smart City» не використовувалося. Перша його згадка була датована в 1991 році, хоча саме словосполучення ще не було дефінітивно визначеним¹⁷⁸. Широкого обігу вказана категорія набула уже в середині 2000-х років. Прийнято вважати, що вперше термін «Smart City» у сучасному розумінні

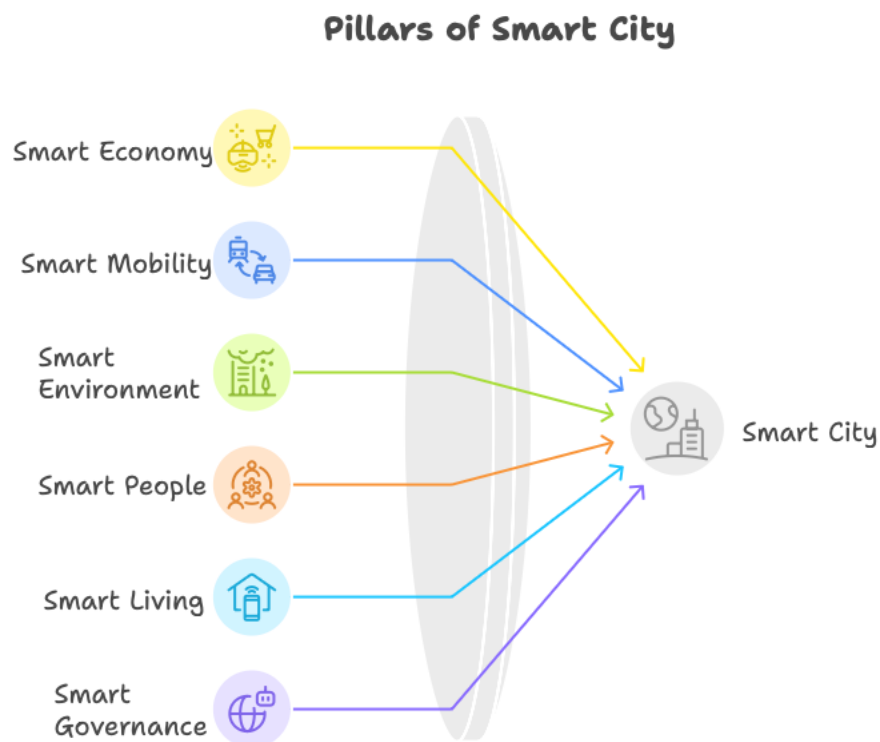
¹⁷⁶ Komninos, N., Tsampoulatidis, I., Kakderi, C., Nikolopoulos, S., & Kompatsiaris, I. Projects for Intelligent and Smart Cities: Technology and Innovation Transforming City Ecosystems // Preprints. 3 серпня 2021. URL: <https://www.preprints.org/manuscript/202108.0080/v1> (date of access: 03.05.2025).

¹⁷⁷ Peter van den Besselaar. *E-community versus e-commerce: The rise and decline of the Amsterdam Digital City* // *AI & Society*, 2001, Vol. 15, No. 3, pp. 280–288. DOI: 10.1007/BF01208709.

¹⁷⁸ Pérez, L. M., Oltra-Badenes, R., Oltra Gutiérrez, J. V., Gil-Gómez, H. A bibliometric diagnosis and analysis about smart cities / L. M. Pérez, R. Oltra-Badenes, J. V. Oltra Gutiérrez, H. Gil-Gómez // *Sustainability*. 2020. Vol. 12, No. 16. Article number: 6357. DOI: <https://doi.org/10.3390/su12166357>.

було вжито в 2007 році. Адже саме тоді група європейських дослідників з Центру регіональних наук Віденського університету технологій (Centre of Regional Science, Vienna University of Technology) на чолі з Рудольфом Гіффінгером опублікувала один із перших рейтингових звітів «Розумні міста – рейтинг середніх міст Європи»¹⁷⁹, де авторський колектив запропонував шість ключових вимірів, які дали чіткі орієнтири для розуміння «розумного» міста (критерії *Smart City*).

Цими *вимірами* є: 1. Розумна економіка; 2. Розумна мобільність; 3. Розумне середовище; 4. Розумні люди; 5. Розумне життя; та 6. Розумне управління¹⁷⁸. Ця модель широко використовується для оцінки ефективності міської політики в країнах ЄС.



«Розумна економіка (Smart Economy)». Вимір «Розумна економіка» відповідає за економічну конкурентоспроможність міста. Він включає

¹⁷⁹ Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. Smart Cities – Ranking of European Medium-Sized Cities / R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanović, E. Meijers. Vienna: Centre of Regional Science, Vienna University of Technology, 2007. URL: https://www.smart-cities.eu/download/smart_cities_final_report.pdf (date of access: 03.05.2025).

інноваційну активність, підприємництво, продуктивність, гнучкість ринку праці, імідж та брендинг міста, а також його інтеграцію в національні й міжнародні ринки. Тобто розвинена розумна економіка – це основа інноваційного зростання і зайнятості, де місцева влада стимулює нові бізнес-моделі (стартапи), впроваджує технологічні інвестиції й залучає іноземні інвестиції.

«Розумна мобільність (Smart Mobility)». Вона стосується транспортної інфраструктури та цифрових технологій (інтелектуальні транспортні системи (ITS – *Intelligent Transport Systems*). Розумна мобільність забезпечує ефективне та екологічно стале пересування мешканців і товарів. За пропонованою моделлю, до цього виміру належать локальна та національна доступність міста (достатня транспортна мережа, сполучення з регіоном і світом), доступність ITS -цифрової інфраструктури для транспорту, а також сучасні та безпечні транспортні системи (наприклад, електромобілі, громадський транспорт, вело- та пішохідні мережі). Тобто місто з розумною мобільністю інтегрує різні види транспорту (громадський, приватний, нелінійні сервіси тощо) у єдину систему, зменшує затори і забруднення завдяки цифровим рішенням та альтернативним видам транспорту.



«Розумне середовище (Smart Environment)». Відображає стійкість і екологічність міста. Цей вимір включає природні умови та управління ресурсами: якість навколишнього середовища, охорону природи, енергоефективність та збереження ресурсів. Модель виділяє такі критерії, як привабливість природних умов (клімат, зелена зона), рівень забруднення, зусилля з охорони довкілля та збалансований обіг ресурсів. Іншими словами, розумне середовище означає, що місто мінімізує негативний вплив на природу – зменшує викиди, впроваджує технології ощадного використання енергії і води, ефективно утилізує відходи тощо.

«Розумні люди (Smart People)». Цей вимір фокусується на соціальному капіталі міста – освіченості, креативності й громадянській участі мешканців. В даному контексті «Розумні люди» – це насамперед освічені та відкриті до навчання мешканці міст, які активно взаємодіють один з одним незалежно від соціального чи етнічного походження. Тобто крім високого рівня освіти, важливими є соціальна згуртованість, гнучкість мислення, творчість та залученість мешканців у громадське життя і процеси прийняття рішень.

«Розумне життя (Smart Living)». Охоплює якість життя та соціальне благополуччя людей. Це культурні, соціальні та побутові аспекти міста, що забезпечують комфортне і безпечне середовище для його мешканців. У рамках моделі це включає інфраструктуру дозвілля та культури (музеї, театри, парки),



Зображення: Pixabay.com

системи охорони здоров'я, житлові умови, освітні заклади, туристичну привабливість та соціальну згуртованість населення. Розумне життя означає, що мешканці мають доступ до якісних послуг, безпеки та культури, що підвищує загальний рівень добробуту.

«Розумне управління (Smart Governance)». Відображає ефективність та прозорість міського управління. Вимір передбачає залучення громадян до прийняття рішень та надання їм доступу до якісних публічних, соціальних послуг. Сюди входять такі аспекти: участь громадян у прийнятті рішень (зворотний зв'язок, петиції, електронні консультації), доступність публічних послуг (цифрові сервіси міської адміністрації), прозора система управління (відкриті дані, публічні бюджети) та стратегічні плани розвитку. Розумне управління означає, що влада координує дії між різними відомствами, використовує інформаційно-комунікативні технології (ІКТ) для підвищення ефективності та взаємодії, а також підтримує довіру жителів міст через підзвітність і інклюзивність публічної влади.

Отримавши базове наукове обґрунтування, у другій половині 2000-х концепція Smart City активно «входить» у фокус уваги міжнародних організацій, урядів провідних країн та всесвітньо відомих технологічних корпорацій. Зокрема, у 2005 році компанія Cisco інвестує \$25 млн у дослідження міських ІТ-рішень¹⁸⁰, а у 2008 році IBM ініціює програму *Smarter Planet*, в якій «розумним» містам приділялася ключова роль. Вже у 2009 році, та ж таки, IBM запускає глобальну кампанію *Smarter Cities* з бюджетом у \$50 млн, просуваючи рішення для підвищення ефективності міського управління¹⁸¹.

Відповідно й уряди провідних країн світу через різноманітні програми почали активно долучатися до просування даної концепції. Так, у США інвестиції в *smart grid* (у перекладі з англ. – «розумна електромережа») були передбачені федеральним Законом про відновлення та реінвестування (American Recovery and Reinvestment Act of 2009)¹⁸². У свою чергу, в Європейському Союзі було ухвалено Директиву 2009/72/ЄС, що зобов'язувала країни-члени до 2020 року забезпечити розумними лічильниками щонайменше 80% споживачів електроенергії¹⁸³.

У цей же період на муніципальному рівні (особливо в країнах ЄС) почали активно розроблятися та впроваджуватися стратегії й програми Smart City, а також відбуватися різноманітні заходи, присвячені питанням розвитку концепції «розумного» міста. Одним із ініціаторів у цій сфері став знову ж таки Амстердам, де у 2009 році була започаткована програма «Amsterdam Smart City»¹⁸⁴ – ініціатива, що об'єднала понад сотню проєктів, спрямованих на енергоефективність, сталу мобільність, цифрову інфраструктуру та інтеграцію

¹⁸⁰ Cisco Systems. Connected Urban Development: Cisco's \$25 Million Investment in Smart City Research. *Information Age*. 2007. URL: <https://www.information-age.com/ibm-cisco-and-the-business-of-smart-cities-26972/> (date of access: 03.05.2025).

¹⁸¹ IBM Corporation. IBM Pledges \$50 Million to Create 100 Smarter Cities. *PR Newswire*. 2010. URL: <https://www.prnewswire.com/news-releases/ibm-pledges-50-million-to-create-100-smarter-cities-106944123.html> (date of access: 03.05.2025).

¹⁸² U.S. Department of Energy. Recovery Act: Smart Grid Investment Grant (SGIG) Program. *Office of Electricity*. 2009. URL: <https://www.energy.gov/oe/recovery-act-smart-grid-investment-grant-sgig-program> (date of access: 03.05.2025).

¹⁸³ European Commission. Smart Metering Deployment in the European Union. *Joint Research Centre*. 2019. URL: <https://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union> (date of access: 03.05.2025).

¹⁸⁴ Amsterdam Smart City. About the Program. 2009. URL: <https://amsterdamsmartcity.com/about> (date of access: 03.05.2025).

інновацій у повсякденне життя міста. Особливістю програми було активне залучення мешканців міста у процес розробки та обговорення рішень, зокрема через використання мобільних додатків для розумного паркування, енергозбереження та міського планування в цілому.

З 2011 року Барселона (Іспанія), започаткувала й до сьогодні щорічно проводить Smart City Expo World Congress (SCEWC)¹⁸⁵ – провідний міжнародний форум з питань урбаністичних інновацій. У рамках реалізації smart-стратегії місто запровадило ряд інновацій: сенсори для управління трафіком, освітленням та сміттям, створило платформи відкритих даних, розширило цифрові послуги для громадян. У цьому ж році (2011) муніципалітет Барселони започаткував низку важливих партнерств з провідними технологічними компаніями, зокрема у межах ініціативи City Protocol¹⁸⁶, щоб з допомогою цифрових технологій стати в майбутньому еталонною моделлю сталого міського розвитку.

Таким чином, кінець 2000-х – початок 2010-х років став періодом стрімкого та широкого утвердження концепції Smart City як у глобальному дискурсі, так власне й регіональній та міській політиці.

2. Еволюція змісту концепції „Smart City“

Закономірно, що з плином часу зміст поняття «розумного» міста зазнав значної трансформації. Якщо спочатку акцент робився передусім на технологічних рішеннях та інфраструктурі, то згодом фокус змістився на питання організації міського управління, партисипативної демократії та принципів сталості (збалансованості) міського розвитку.

Загалом науковці виділяють кілька ключових етапів або «поколінь» розвитку концепції *Smart City*. Так, американський урбаніст, всесвітньо відомий

¹⁸⁵ Fira de Barcelona. Smart City Expo World Congress. 2024. URL: <https://www.smartcityexpo.com/> (date of access: 03.05.2025).

¹⁸⁶ Cisco Systems. Barcelona and Cisco Announce Strategic Initiatives to Transform the City into a Global Urban Reference Model. 2012. URL: <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2012/m03/barcelona-and-cisco-announce-strategic-initiatives-to-transform-the-city-into-a-global-urban-reference-model.html> (date of access: 03.05.2025).

дослідник сталого міського розвитку, Бойд Кoen, описує три хвилі еволюції «розумних» міст¹⁸⁷: Smart City 1.0 – початковий етап, коли ініціатива надходила переважно від приватних компаній, які пропонували впровадження технологічних цифрових рішення без активної участі міської влади або громадськості; Smart City 2.0 – наступний етап, коли спостерігається активізація муніципальної влади щодо визначення потреб та впровадження цифрових технологій для покращення різних аспектів якості життя в межах міського середовища (цифрові технології стають інструментом, підпорядкованим цілям міського розвитку); Smart City 3.0 – це сучасний етап розвитку концепції «розумного» міста, що робить акцент на демократії участі (активній співтворчості з жителями міст), зокрема їх широкому залученні до обговорення та розробки важливих рішень, пріоритизації вирішення міських проблем з допомогою цифрових технологій, а також реалізації ініціатив, спрямованих на сталий міський розвиток, соціальну справедливість та інклюзію.

Фактично третє покоління Smart City (3.0) ставить людину в центр своїх пріоритетів. У ньому беруть участь громадяни, які шляхом формування різних форм соціальної комунікації долучаються до співуправління містом¹⁸⁸. Основним проявом цієї взаємодії є соціальна участь – процес, що реалізується за допомогою різноманітних інструментів, через які представники суспільства впливають на рішення органів місцевого самоврядування, що безпосередньо або опосередковано стосуються їхніх інтересів¹⁸⁹.

Таким чином, якщо в першому поколінні розуміння концепту *Smart City* переважала, так би мовити, технократична перспектива (віра в те, що впровадження «розумних» систем автоматично покращить місто), то в другому поколінні з'явилося розуміння необхідності відповідних законодавчих та інституційних змін, зокрема щодо відкритих даних та прозорості. Коли в

¹⁸⁷ Cohen, B. The 3 Generations of Smart Cities. *Fast Company*. 2015. URL: <https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities> (date of access: 03.05.2025).

¹⁸⁸ Giela M. The Human Element in the Context of Smart Cities Management Systems. *Management Systems in Production Engineering*. 2023. Vol. 31, № 3. P. 301–307. DOI: 10.2478/mspe-2023-0033.

¹⁸⁹ D. Długosz and J.J. Wygnański, Obywatele współdecydują. Przewodnik po partycypacji społecznej, Warszawa: Stowarzyszenie na Rzecz Forum Inicjatyw Pozarządowych, p. 11, 2005

третьому поколінні прийшло усвідомлення того, що без активної участі громади та врахування прав людини місто не може бути по-справжньому «розумним».

Цікаво, що науковці виокремлюють наступну хвилю розвитку концепції Smart City. На цьому тлі сучасна Smart City 4.0¹⁹⁰ постає як системна інтеграція трьох попередніх хвиль, у межах якої технології, публічно-владні інституції та люди об'єднуються в платформну, сталу та етично орієнтовану цифрову екосистему. Її визначальними характеристиками є взаємозв'язок усіх учасників міського життя, використання великих даних та штучного інтелекту для прийняття управлінських рішень, пріоритет сталого міського розвитку, а також етика цифрового міського середовища. У результаті, поняття «розумного міста» переходить від фокусування на технологічних інноваціях до багатовимірної концепції, в центрі якої – людина, взаємодія та довіра.

Еволюція концепції "Smart City"



З огляду на вказану вище інформацію, якщо поставити запитання «Яким повинне бути прогресивне та успішне місто майбутнього?», то одна з найцікавіших відповідей звучить так: таке місто повинне виражати синтез трьох невід'ємних компонентів – «тіла, розуму і душі». «Тіло» – це інфраструктура, що втілює фізичний простір і технічні системи міста; «розум» – це цифрові технології та програмне забезпечення, які забезпечують управління даними,

¹⁹⁰ Giffinger R., Haindlmaier G., Kramar H. European Smart Cities 4.0. Vienna University of Technology, 2021. URL: <https://smart-cities.eu/?cid=01&ver=4> (date of access: 03.05.2025).

сервісами, мобільністю; «душа» – це людський вимір, що об'єднує бачення, креативність, співпрацю та цінності спільноти¹⁹¹.

Ця метафора вдало резонує з вказаною вище еволюцією чотирьох поколінь концепції Smart City, яку можна інтерпретувати наступним чином: *Smart City 1.0* зосереджується переважно на технологічному «тілі» міста – інфраструктурі, яку формують великі ІТ-корпорації, впроваджуючи інноваційні рішення зверху вниз; *Smart City 2.0* надає місту «розуму»: у цьому підході ініціатива переходить до муніципалітетів, які за допомогою цифрових технологій визначають пріоритети розвитку та підвищують ефективність управління; *Smart City 3.0* та *4.0* розкриває, так би мовити, «душу» міста – через залучення жителів до співтворчості, спільного генерування рішень, а також реалізації ідей соціальної справедливості, інклюзії та сталості.

Очевидно, що одним із ключових викликів для сучасного міського розвитку є здатність гармонійно поєднати ці три елементи – технології, управління та людський потенціал – в єдину, цілісну систему, яка працює в інтересах громади та формує життєздатне, інклюзивне і адаптивне місто майбутнього.

Слід зазначити, що синхронно з еволюцією практичної сторони реалізації концепції «розумного» міста через розширення її функціонального призначення змінювався також і акцент у визначеннях. Адже ранні визначення часто підкреслювали економічну конкурентоспроможність та впровадження ІКТ, тоді як пізніші почали включати питання екології, якості життя, а також забезпечення сталого (збалансованого) міського розвитку.

Цілком справедливо критики техноцентричного підходу звернули увагу на те, що «розумність» міста має вимірюватися не лише кількістю впроваджених технологій, а й тим, наскільки вони приносять реальну користь жителям міста, забезпечують рівність, а також сприяють покращенню муніципального

¹⁹¹ World Economic Forum. Building a Digital Infrastructure: Issues and Opportunities. Geneva: World Economic Forum USA, 2015. 24 p. URL: https://www3.weforum.org/docs/WEFUSA_DigitalInfrastructure_Report2015.pdf (date of access: 03.05.2025).

врядування¹⁹². Власне ці об'єктивні зауваження і сприяли перегляду концепції. Нині поняття «*Smart City*» дедалі більше охоплює такі аспекти, як участь жителів міста у прийнятті рішень (*smart governance*), розвиток людського капіталу (*smart people*), екологічна стійкість (*smart environment*) та інтегроване планування простору (*smart living*).

Отже, еволюція *Smart City* – це перехід від вузького розуміння «місто як сукупність гаджетів» до ширшого бачення «місто як платформа співпраці влади, громадянського суспільства і бізнесу на основі даних» з метою забезпечення сталого міського розвитку. Такий підхід цілком відображає зрілість концепції. Безсумнівно, справді «розумне» місто вимагає не лише нових технологій, але й інновацій у самій структурі міського врядування, в тому числі через удосконалення муніципальних нормативно-правових основ.

Міжнародні організації та провідні експертні платформи подають концепцію *Smart City* як багатогранну, орієнтовану на людину модель міського розвитку, що ґрунтується на ефективному використанні цифрових та інформаційно-комунікаційних технологій.

Згідно з документами Європейської Комісії, «розумне» місто – це місце, де традиційні мережі та послуги стають ефективнішими завдяки цифровим технологіям та ІКТ, працюючи на благо жителів і бізнес-спільноти. Мова йде не лише про ефективніше використання ресурсів і зменшення викидів, але також про розумні транспортні мережі, модернізовані системи водопостачання, поводження з відходами, ефективне освітлення та опалення будівель, безпечні публічні простори, інтерактивне врядування і реагування на потреби старіючого населення¹⁹³.

Підхід до розуміння «розумного» міста в рамках діяльності ООН пов'язаний з цифровізацією, використанням чистої енергії та впровадженням *smart*-технологій, зокрема у транспорті. Його мета – надати змогу жителям

¹⁹² Hollands, R. G. Will the real smart city please stand up? *City*. 2008. Vol. 12, No. 3. P. 303–320. DOI: 10.1080/13604810802479126.

¹⁹³ European Commission. Smart Cities: Cities using technological solutions to improve the management and efficiency of the urban environment URL: https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en (date of access: 03.05.2025).

міст робити екологічно відповідальний вибір, стимулювати сталу економічну діяльність і покращувати доступ до публічних послуг¹⁹⁴.

За визначенням Британського інституту стандартів (BSI), «розумне» місто – це «ефективна інтеграція фізичних, цифрових та людських систем у міському середовищі для забезпечення сталого, процвітаючого та інклюзивного майбутнього для громадян»¹⁹⁵.

У свою чергу, Міжамериканський банк розвитку (IDB) інтерпретує Smart-місто як інноваційне місто, що використовує ІКТ та інші інструменти для підвищення якості життя, ефективності роботи та конкурентоспроможності, задовольняючи потреби теперішнього і майбутніх поколінь у економічному, соціальному й екологічному вимірах¹⁹⁶.

Провідна міжнародна організація «Smart Cities Council» (SCC) зазначає, що «розумне» місто – це система, яка збирає дані з пристроїв і сенсорів, вбудованих у вулиці, електромережі, будівлі та іншу інфраструктуру¹⁹⁷.

Згідно з позицією не менш відомої європейської організації «Local Governments for Sustainability» (ICLEI), розумні міста – це ті, що інтегрують ефективність використання ресурсів, технологічний прогрес і належне міське врядування задля досягнення ширшого бачення сталого розвитку міст і громад¹⁹⁸. ICLEI розглядає концепцію Smart City як частину ширшого підходу до сталого міського розвитку, де цифрові технології є інструментом для досягнення цілей сталості, інклюзії та кліматичної нейтральності.

¹⁹⁴ UN-Habitat, United Nations. New Urban Agenda. United Nations: UN-Habitat, 2016. URL: <https://nua.unhabitat.org/> (date of access: 03.05.2025).

¹⁹⁵ British Standards Institution. Smart city framework – Guide to establishing strategies for smart cities and communities (PAS 181:2014). London: BSI, 2014. URL: <https://www.bsigroup.com/LocalFiles/en-GB/smart-cities/resources/BSI-Making-cities-smarter-Guide-for-city-leaders-UK-EN.pdf> (date of access: 03.05.2025).

¹⁹⁶ Inter-American Development Bank. The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City. Washington, D.C.: IDB, 2016. URL: <https://publications.iadb.org/publications/english/document/The-Road-toward-Smart-Cities-Migrating-from-Traditional-City-Management-to-the-Smart-City.pdf> (date of access: 03.05.2025).

¹⁹⁷ Smart Cities Council. Definition of a Smart City. URL: <https://smartcitiescouncil.com> (date of access: 03.05.2025).

¹⁹⁸ ICLEI – Local Governments for Sustainability. Smart Cities. URL: <https://iclei-europe.org/topics/smart-cities/> (date of access: 03.05.2025).

Як бачимо, єдиного уніфікованого визначення цього поняття досі не існує. Втім, спільним у сучасних підходах є уявлення про місто, яке завдяки цифровим засобам та інноваціям стає більш ефективним, орієнтованим на потреби сучасного та майбутніх поколінь. Таке розуміння концепції *Smart City* суттєво виходить за межі техноцентризму. У центрі моделі знаходиться індивід та міська громада, а технології виступають засобом досягнення сталого, інклюзивного й ефективного міського розвитку. При цьому ключовими його рисами є: інтегрованість, орієнтація на потреби мешканців міста, прозоре та інклюзивне врядування, розвинута цифрова інфраструктура та соціальна відповідальність.



Один із прикладів реалізації концепції "Smart City".

Bosco Verticale, Milano, Italy

3. Політико-правовий вимір концепції „Smart City“

З широкою популяризацією ідей та принципів *Smart City* виникла потреба в належному їх політичному та правовому закріпленні. На глобальному рівні концепція знайшла відображення у кількох ключових документах.

У Порядку денному ООН у сфері сталого розвитку на період до 2030 року, затвердженому Резолюцією Генеральної Асамблеї ООН A/RES/70/1 від 25 вересня 2015 року¹⁹⁹, окреслено 17 цілей сталого розвитку (ЦСР). В контексті даної тематики на особливу увагу заслуговують цілі № 9 та № 11. Так, Ціль № 11 спрямована на те, щоб «зробити міста і населені пункти відкритими, безпечними, життєздатними і стійкими», коли Ціль № 9 – на «створення стійкої

¹⁹⁹ Порядок денний у сфері сталого розвитку на період до 2030 року=Transforming Our World: The 2030 Agenda for Sustainable Development : резолюція, прийнята Генеральною Асамблеєю ООН 25 вересня 2015 року, A/RES/70/1. Нью-Йорк : ООН, 2015. 41 с. URL: <https://sdgs.un.org/2030agenda> (дата звернення: 03.05.2025).

інфраструктури, сприяння інклюзивній та стійкій індустріалізації та інноваціям». Обидві цілі опосередковано охоплюють завдання цифрової трансформації міської інфраструктури, зокрема через впровадження інтелектуальних технологій, розвиток цифрових сервісів для населення та модернізацію управлінських процесів на рівні муніципалітетів. Таким чином, концепція «розумного» міста стала набувати дедалі більшого (глобального) значення як інструмент досягнення ЦСР в урбанізованих просторах.

У 2016 році на Конференції ООН з питань житлового господарства та сталого розвитку (Habitat III) було прийнято «Новий міський порядок денний» (New Urban Agenda), який закликав до використання інноваційних технологій задля інклюзивного та сталого урбаністичного розвитку. У документі (пункт 66) зазначено: «Ми зобов'язуємося дотримуватися підходу «розумного міста», що передбачає використання можливостей цифровізації, екологічно чистої енергії, новітніх технологій та інноваційного транспорту. Це дозволить мешканцям обирати більш екологічно сталий спосіб життя, сприятиме сталому економічному зростанню та підвищенню якості надання міських послуг»²⁰⁰.

Також спеціалізовані установи ООН активно долучилися до напрацювання відповідних рекомендацій. Зокрема Міжнародний союз електрозв'язку (ITU) спільно з регіональними комісіями ООН (UNECE) у 2016 р. започаткував ініціативу U4SSC (United for Smart Sustainable Cities)²⁰¹, в рамках якої було розроблено універсальні показники ефективності для Smart City та опубліковано низку настанов та рекомендацій для міст. Згодом результатом цієї роботи стали міжнародні стандарти ISO серії 37100, що визначають індикатори сталого розвитку громад і розумних міст (наприклад, стандарт ISO 37122:2019 «Індикатори для розумних міст» та ISO 37106:2018 «Стійкі міста та громади» (згодом оновлений до ISO 37106:2021 «Сталий розвиток міст і громад. Настанови

²⁰⁰ Нова міська програма=New Urban Agenda : прийнята на Конференції ООН з питань житлового господарства та сталого розвитку (Habitat III), Кіто, Еквадор, 17–20 жовтня 2016 р. Нью-Йорк : Організація Об'єднаних Націй, 2017. 72 с. URL: <https://habitat3.org/the-new-urban-agenda> (дата звернення: 03.05.2025).

²⁰¹ United for Smart Sustainable Cities (U4SSC) : глобальна ініціатива, започаткована Міжнародним союзом електрозв'язку (ITU), Європейською економічною комісією ООН (UNECE) та Програмою ООН з населених пунктів (UN-Habitat) у 2016 році. Женева : ITU, 2016. URL: <https://u4ssc.itu.int> (date of access: 03.05.2025).

щодо створення операційних моделей розумного міста для сталих громад»)²⁰². Хоч ці стандарти не становлять загально-обов'язкового характеру, вони стали важливими орієнтирами та власне інструментами оцінювання для муніципалітетів по всьому світу.

Окрім вищевказаних стандартів, на міжнародному рівні також приймалися і так звані «м'які» нормативні акти (*soft law*), положення яких спрямовувалися на формування та розвиток «розумних» міст. У 2019 році в межах співпраці країн «Великої двадцятки» (G20) було започатковано глобальну ініціативу у сфері розумних міст – *Global Smart Cities Alliance*, яка діє під егідою Всесвітнього економічного форуму²⁰³. Діяльність *Global Smart Cities Alliance* є показовою щодо становлення правового виміру концепції *Smart City*, оскільки визначає глобальні нормативні орієнтири для етичного управління цифровими технологіями в міському середовищі. Це сприяє формуванню загальновизнаних стандартів прозорості, відповідальності та захисту прав людини в процесі розвитку smart-інфраструктури.

У 2023 році Програма ООН з населених пунктів (UN-Habitat) під егідою Асамблеї ООН-Хабітат ініціювала розробку Міжнародних керівних принципів щодо «розумних» міст, пріоритетно орієнтованих на людей. Це рамкові рекомендації (*non-binding guidelines*), покликані допомогти країнам і містам створювати власні політики і механізми реалізації ідей *Smart City*, з допомогою яких цифрова інфраструктура та дані слугували б інтересам сталості, інклюзивності та правам людини. За твердженням ініціаторів даних принципів,

²⁰² ISO 37122:2019. Сталий розвиток міст і громад. Індикатори для розумних міст = *Sustainable cities and communities — Indicators for smart cities*. Женева : Міжнародна організація зі стандартизації, 2019. 56 с. URL: <https://www.iso.org/standard/69050.html> (date of access: 03.05.2025); ISO 37106:2018. Сталий розвиток міст і громад. Настанови щодо створення операційних моделей розумного міста для сталих громад = *Sustainable cities and communities — Guidance on establishing smart city operating models for sustainable communities*. Женева : Міжнародна організація зі стандартизації, 2018. 40 с. URL: <https://www.iso.org/standard/62065.html> (date of access: 03.05.2025); ISO 37106:2021. Сталий розвиток міст і громад. Настанови щодо створення операційних моделей розумного міста для сталих громад = *Sustainable cities and communities — Guidance on establishing smart city operating models for sustainable communities*. Женева : Міжнародна організація зі стандартизації, 2021. 57 с. URL: <https://www.iso.org/standard/62065.html> (date of access: 03.05.2025).

²⁰³ World Economic Forum. *Global Smart Cities Alliance*. URL: <https://www.globalsmartcitiesalliance.org/about> (date of access: 03.05.2025).

вони також скеровувалися на заповнення глобальних «нормативних прогалів» у сфері цифрового розвитку міст²⁰⁴.

На рівні Європейського Союзу концепція *Smart City* також широко інтегрована до різномісцевих стратегічних документів та програм розвитку, хоча спеціалізованого окремого «закону про розумні міста» в ЄС немає. Стимулюючим фактором поширення відповідної концепції свого часу стала загальна стратегія «Європа 2020», ухвалена у березні 2010 році, яка визначила пріоритети «розумного, сталого та інклюзивного зростання»²⁰⁵. Однією з семи флагманських ініціатив цієї стратегії стала «Цифрова програма для Європи» (*Digital Agenda for Europe*), офіційно представлена 19 травня 2010 року²⁰⁶. Її метою було максимізувати соціальний та економічний потенціал інформаційно-комунікаційних технологій (ІКТ), зокрема Інтернету, шляхом створення єдиного цифрового ринку, розвитку широкосмугового доступу, підвищення цифрової грамотності та забезпечення довіри людей до цифрових технологій.

Хоча *Digital Agenda for Europe* не створювала прямої нормативно-правової бази для розвитку *Smart City*, водночас вона визначила стратегічну основу для майбутньої (проспективної) правотворчості, що згодом трансформувалася у різні нормативні акти ЄС²⁰⁷. Таким чином, цей документ опосередковано вплинув на правові аспекти розвитку розумних міст у Європі.

²⁰⁴ UN-Habitat to draft people-centred smart city regulations. *SmartCitiesWorld*. 22 квітня 2024. URL: <https://www.smartcitiesworld.net/policymaking/un-habitat-to-draft-people-centred-smart-city-regulations> (date of access: 03.05.2025).

²⁰⁵ European Commission. Europe 2020. A strategy for smart, sustainable and inclusive growth. *EUR-Lex*. 2010. COM(2010) 2020 final. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF> (date of access: 03.05.2025).

²⁰⁶ European Commission. A Digital Agenda for Europe. *EUR-Lex*. 2010. COM(2010) 245 final. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> (date of access: 03.05.2025).

²⁰⁷ Європейський парламент; Рада ЄС. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (date of access: 03.05.2025); Європейський парламент; Рада ЄС. 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 (eIDAS Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> (date of access: 03.05.2025); Європейський парламент; Рада ЄС. 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). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (date of access: 03.05.2025); Європейський парламент; Рада ЄС. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/868/oj> (date of access: 03.05.2025) і ін.

Важливим правовим чинником юридизації ініціатив Smart City стала реформа законодавства ЄС у сфері захисту персональних даних, яка знайшла своє втілення в ухваленні Загального регламенту про захист даних (GDPR), що набув чинності у 2018 році²⁰⁸. Положення Регламенту суттєво вплинули на всі проекти, пов'язані зі збором персональних даних жителів міст країн-членів ЄС. Він встановив чіткі вимоги щодо прозорості, погодження та безпеки обробки даних. Тож міста, що впроваджують системи моніторингу (камери, датчики, сенсори тощо), зобов'язані забезпечувати неухильне дотримання цих вимог.

Наприклад, якщо збираються відеодані чи інша інформація про мешканців міст, потрібне правове обґрунтування і обов'язкове повідомлення про це громадськості. Свого часу в одному із міст Італії спроба запровадити систему розпізнавання обличч у громадських місцях наštтовхнулася на вимогу національного органу із захисту даних надати детальне обґрунтування та оцінку впливу, а через відсутність належної правової бази – була заборонена до реалізації²⁰⁹. Цей випадок підтверджує, що *smart*-технології в містах Європи діють в межах жорстких нормативно-правових обмежень, які покликані, перш за все, захистити права людини.

На європейському рівні розробляються й інші положення із визначеними стандартами та технічними рекомендаціями для «розумних» міст. Зокрема європейські органи стандартизації CEN-CENELEC та ETSI у 2020 році видали низку актів, як-от ETSI TR 103 455 (2020)²¹⁰ щодо стандартів інфраструктури «розумних» міст. Такі документи класифікують дані, протоколи зв'язку, інтероперабельність систем, що полегшує взаємодію різних постачальників цифрових рішень на ринку *Smart City*. Таким чином, на рівні ЄС нормативно-

²⁰⁸ Європейський парламент; Рада ЄС. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (date of access: 03.05.2025).

²⁰⁹ Pagallo, Ugo. Smart Cities and the GDPR: The Role of the Data Protection Impact Assessment. *Smart Cities*. 2023. Vol. 6, No. 1. Article 27. DOI: <https://doi.org/10.3390/smartcities6010027> URL: <https://www.mdpi.com/2624-6511/6/1/27>

²¹⁰ European Telecommunications Standards Institute (ETSI). TR 103 455 V1.1.1 (2020-11): SmartM2M; Smart Cities and Communities; Standards landscape and gap analysis. 2020. 60 с. URL: https://www.etsi.org/deliver/etsi_tr/103400_103499/103455/01.01.01_60/tr_103455v010101p.pdf (date of access: 03.05.2025).

правове поле навколо концепції *Smart City* є багаторівневим: від глобальних цілей і принципів – до конкретних стандартів і регуляцій ЄС, які забезпечують збалансований розвиток технологій з дотриманням прав мешканців.

З огляду на це, поширення *Smart City* ініціатив також суттєво впливає на розвиток муніципального права та практику місцевого самоврядування в країнах ЄС. По-перше, воно стимулює впровадження принципів цифрового врядування (*e-governance*) на місцевому рівні. Європейські міста, що прагнуть бути «розумними», переглядають свої нормативні акти, щоб забезпечити якісне надання електронних послуг, електронного документообігу, використання електронної ідентифікації людини (наприклад, для доступу до міських сервісів). Це вимагає прийняття відповідних локальних актів про електронні петиції, електронні звернення, регулювання роботи порталів відкритих даних тощо. У результаті формується новий пласт муніципального законодавства, що регулює цифрову інфраструктуру міста – від правил розміщення датчиків і мереж 5G до порядку використання міських платформ спільного користування.

По-друге, *Smart City* піднімає питання розширення правового статусу людини у цифровому середовищі міста. Адже жителі міст є не лише пасивними отримувачами публічних послуг. Вони стають активними учасниками збору даних (через смартфони, носимі пристрої), співавторами рішень (через платформи електронної демократії) та співвиконавцями окремих функцій (наприклад, сповіщення місцевої влади про ті чи інші проблеми через додатки). Це вимагає забезпечення належної реалізації існуючих та закріплення нових прав та обов'язків: права на доступ до інформації, права на приватність у місті, права на підключення до Інтернету, обов'язків дотримуватися правил користування спільними цифровими ресурсами тощо.

Багато міст Європи та світу вже проголосили доктрини так званих «цифрових прав» людини. Так, у 2018 році Барселона (Іспанія), Амстердам (Нідерланди) та Нью-Йорк (США) ініціювали *Коаліцію міст за цифрові права*²¹¹,

²¹¹ Open & Agile Smart Cities. Amsterdam, Barcelona and New York City launch global coalition to protect digital rights. *Open & Agile Smart Cities*. 2018. URL: <https://oascities.org/amsterdam-barcelona-and-new-york-city-launch-global-coalition-to-protect-digital-rights/> (date of access: 03.05.2025).

прийнявши декларацію з п'яти базових принципів – доступність інтернету для всіх, захист приватності й персональних даних, прозорість і підзвітність алгоритмів, сприяння участі громади у прийнятті рішень, відкриті та етичні стандарти цифрових послуг. Ці принципи, підтримані ООН-Хабітат, тепер служать еталоном для муніципалітетів усього світу щодо того, як впроваджувати технології без порушення прав людини.

Крім того, концепція *Smart City* актуалізує проблему захисту персональних даних в муніципальному управлінні. Адже «розумні» міста генерують величезні обсяги даних про мешканців – пересування транспортом, споживання енергії, користування послугами, зображення з камер спостереження тощо. Для муніципальної влади це означає необхідність розробки локальних політик щодо використання даних: правил анонімізації інформації, умов передачі даних приватним партнерам, строків зберігання записів з відеокamer, процедур реагування на витоки інформації. Містам доводиться створювати посади уповноважених з питань захисту даних, укладати договори з ІТ-компаніями з урахуванням вимог про *privacy-by-design* (конфіденційність за замовчуванням) тощо. Невиконання цих вимог може призвести до юридичної відповідальності муніципалітетів та підрядників згідно із законодавством про захист інформації.

Паралельно постають і питання кібербезпеки: від безпеки smart-систем залежить не лише інформація, а й різні процеси (наприклад, управління світлофорами чи електромережею), тому європейські міста змушені ухвалювати відповідні локальні акти та плани дій для протидії кіберзагрозам на місцевому рівні, що раніше не входило до їх традиційної сфери регулювання.

Важливим аспектом є вплив *Smart City* на розвиток інструментів електронної демократії. «Розумні» міста використовують технології для залучення громади – онлайн-платформи громадського бюджету, електронні консультації щодо містобудівних планів, додатки для повідомлення про проблеми (ями на дорогах, непрацюючі ліхтарі) тощо. Це спонукає органи місцевого самоврядування врегульовувати право жителів міст на участь через цифрові канали. Наприклад, міста ухвалюють положення про проведення електронних

громадських слухань або запроваджують легальні механізми врахування результатів електронних опитувань у рішеннях ради.

Отже, *Smart City* розширює можливості реалізації конституційних прав на участь в управлінні на місцевому рівні, проте одночасно вимагає гарантій проти зловживань (ідентифікація учасників, запобігання маніпуляціям, забезпечення



Фото: Kostiantyn Stupak, Pexels.com

інклюзивності для тих, хто не має доступу до інтернету). У відповідь на ці виклики в містах з'являються нові норми «м'якого» права – етичні кодекси використання штучного інтелекту в публічних послугах, хартії відкритих даних, угоди про партнерство з ІТ-бізнесом, що встановлюють межі використання даних громади.

В контексті вищевказаного вартий особливої уваги приклад «розумних» міст ФРН. Безпосередньо у німецьких містах концепція «*Smart City*» розробляються з урахуванням локальних особливостей та стратегічних пріоритетів, що зумовлює різноманітність підходів.

Так, для прикладу концепція міста Штутгарт («*Smart City Konzept Stuttgart*»)²¹² орієнтована на розвиток інтелектуальної мобільності, цифрової інфраструктури та відкритих даних з акцентом на екологічну стійкість і кліматичну нейтральність. Мюнхен («*Smarter Together – Smart City in Munich*»)²¹³ робить наголос на інтеграцію цифрових адміністративних послуг, смарт-

²¹² Stadt Stuttgart. Smart City Konzept Stuttgart 2022. URL: <https://www.stuttgart.de/medien/ibs/smart-city-konzept-en.pdf> (date of access: 03.05.2025).

²¹³ City of Munich. Smarter Together – Smart City in Munich. URL: https://big-data-test-infrastructure.ec.europa.eu/smarter-together-smart-city-munich_en (date of access: 03.05.2025).

енергетику та штучний інтелект для оптимізації міського управління. Особливістю Гамбурга («mySMARTLife Hamburg») ²¹⁴ є цифровізація портової інфраструктури («SmartPORT») та широке використання IoT-технологій для управління ресурсами та мобільністю. Концепція Дрездена («Smart City Strategy – Projects») ²¹⁵ підкреслює значення інновацій у сфері IoT-рішень, кібербезпеки та цифрової стійкості міста. Водночас Ульм («Zukunftsstadt 2030») ²¹⁶ реалізує платформу «Zukunftsstadt Ulm 2030» з особливим акцентом на залученні мешканців до управління містом через відкриті дані, інклюзивність та інтегровані екологічні проекти. Незважаючи на спільні риси, такі як цифровізація інфраструктури та розвиток смарт-мобільності, стратегії зазначених міст мають істотні відмінності у пріоритетних напрямках і механізмах реалізації концепції Smart City, зумовлені специфікою соціально-економічних, інфраструктурних та екологічних умов кожного міста.

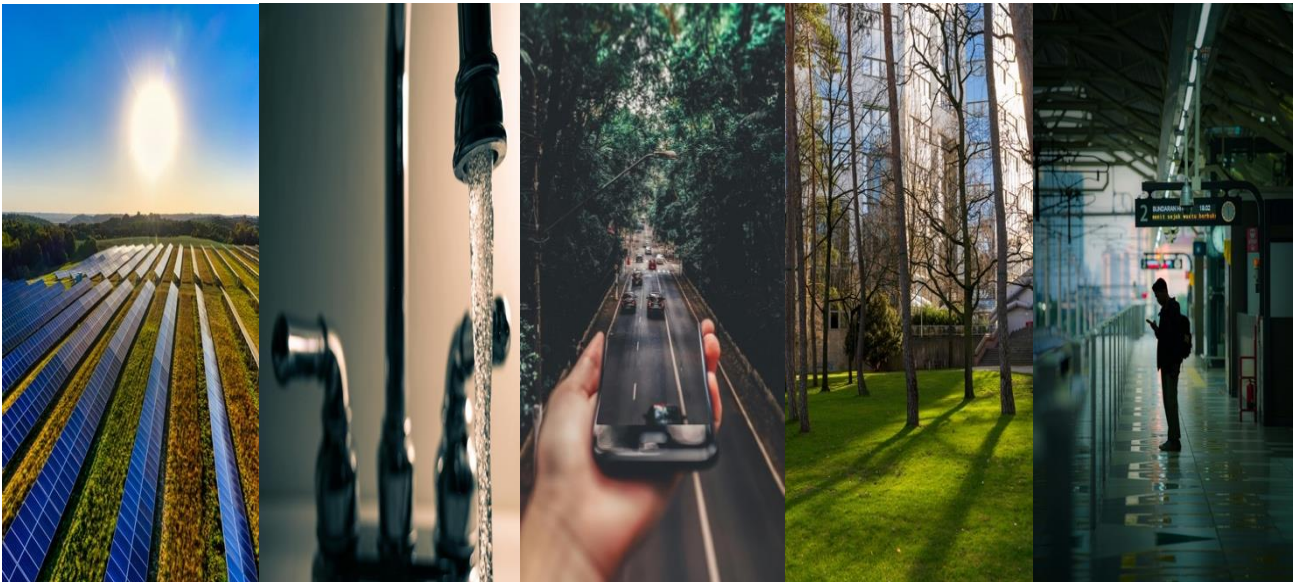


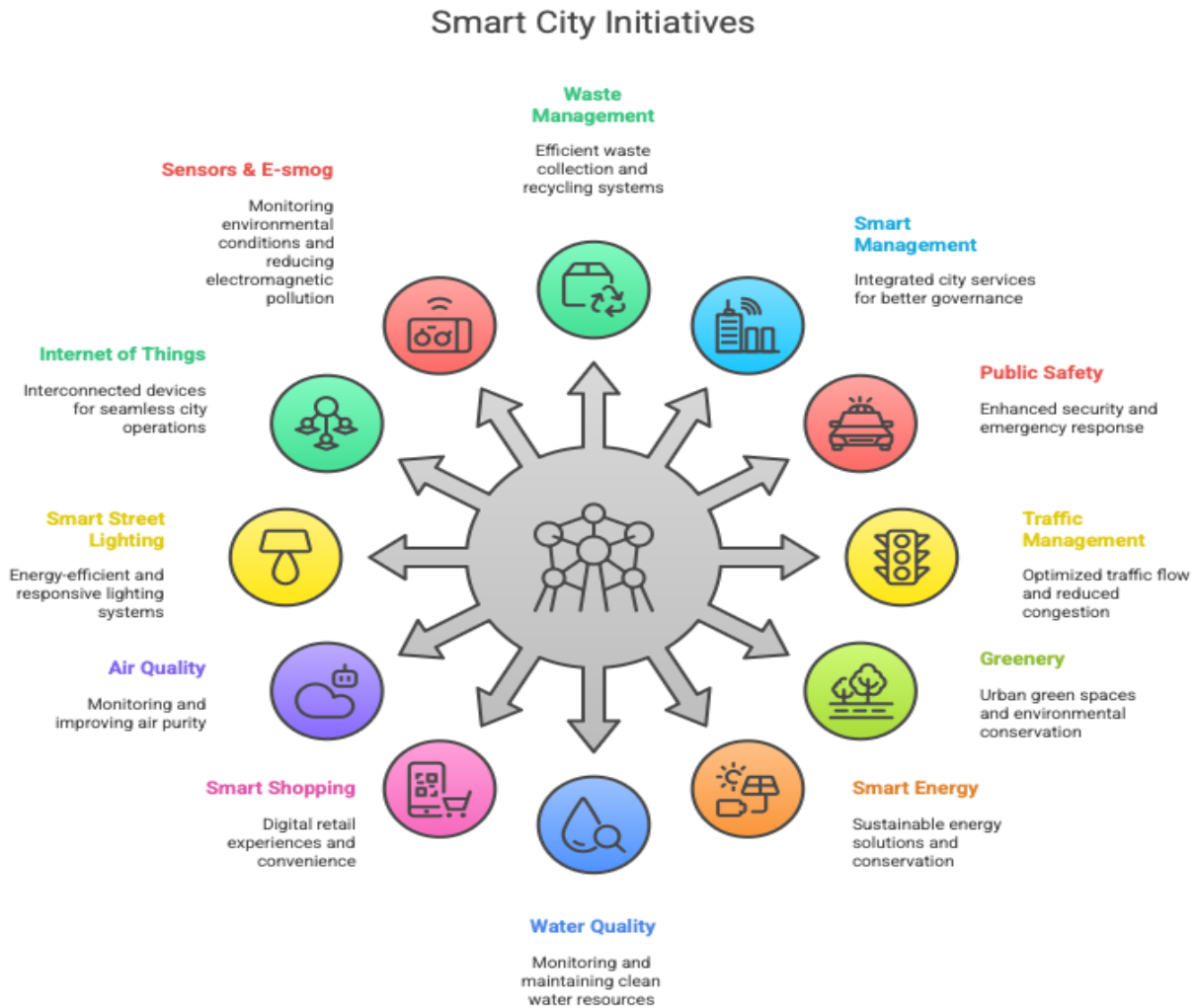
Фото: Tom Fisk, Steve Johnson, Matheus Bertelli, Mohamed B., El Jusuf, Pexels.com

²¹⁴ Smart Cities Marketplace. mySMARTLife Hamburg. URL: <https://smart-cities-marketplace.ec.europa.eu/projects-and-sites/projects/mysmartlife/mysmartlife-hamburg> (date of access: 03.05.2025).

²¹⁵ Smart City Dresden. Smart City Strategy – Projects. URL: <https://smartcity.dresden.de/en/projects/smart-city-strategy> (date of access: 03.05.2025).

²¹⁶ Stadt Ulm. Zukunftsstadt 2030. URL: <https://www.ulm.de/leben-in-ulm/digitale-stadt/zukunftsstadt2030> (date of access: 03.05.2025).

У схемі представлені узагальнені, але не вичерпні ініціативи Smart City.



Слід зазначити, що юридична природа стратегій Smart City у німецьких містах характеризується як документи програмно-концептуального (політико-правового) характеру. Це означає, що вони є не нормативно-правовими актами в класичному розумінні (тобто не містять прямої норми права, обов'язкової до виконання всіма суб'єктами), а радше стратегічними програмами або політичними деклараціями, що визначають основні напрями, цілі та пріоритети місцевої політики розвитку міста.

Проте їх юридична значущість не є декларативною. Попри те, що ці стратегії формально не встановлюють обов'язкових юридичних норм, вони здійснюють істотний вплив на формування місцевої політики (визначають напрями витрачання бюджетних коштів, прийняття рішень органами місцевого самоврядування); планування та фінансування проєктів (забезпечують

юридичну основу для фінансової підтримки проєктів із федеральних чи земельних бюджетів); впровадження конкретних нормативно-правових актів (сприяють розробці та ухваленню конкретних регуляторних актів на муніципальному рівні, таких як статuti чи розпорядження).

Інша ситуація із місцевими статутами (Gemeindesatzungen), які у системі права ФРН є нормативно-правовими актами муніципального рівня, що ухвалюються органами місцевого самоврядування (зокрема, муніципальними радами). Їх правова природа визначається тим, що вони містять юридично обов'язкові правила поведінки, які поширюються на територію відповідної громади й регулюють питання місцевого значення, зокрема щодо планування, забудови, благоустрою, комунального господарства, транспорту, екологічних стандартів, а також цифровізації та впровадження концепцій «Smart City».

Серед місцевих статутів (Gemeindesatzungen), які ілюструють практичну реалізацію концепції Smart City у Німеччині, варто відзначити кілька цікавих прикладів. Зокрема, у Кельні діє статут про відкриті дані (Open-Data-Satzung)²¹⁷, що встановлює юридичну основу для збору та поширення муніципальних даних, сприяючи прозорості управління й розвитку інновацій. У Мюнхені важливим є статут про електромобільність (Elektromobilitätssatzung)²¹⁸, який регламентує створення відповідної інфраструктури та стимулює перехід міста на екологічний транспорт. Гамбург затвердив статут про цифрове будівництво (Digitale Bauordnung)²¹⁹, що впроваджує цифрові технології у сфері містобудування та сприяє розвитку «розумних» будівель. Ульм, своєю чергою, активно використовує статут про цифрову участь громадян (Digitale Beteiligungssatzung)²²⁰, завдяки чому мешканці міста мають можливість активно залучатися до управлінських процесів через цифрові платформи.

²¹⁷ Stadt Köln. Urheber- und Nutzungsrechte, Open Data. URL: <https://www.stadt-koeln.de/artikel/06228/index.html> (date of access: 03.05.2025).

²¹⁸ Landeshauptstadt München. Neufassung vom 04.09.2024 URL: <https://risi.muenchen.de/risi/dokument/v/8656965> (date of access: 03.05.2025).

²¹⁹ Behörde für Stadtentwicklung und Wohnen Hamburg. Digitales Baugenehmigungsverfahren – Bauantrag 2.0 URL: <https://www.hamburg.de/politik-und-verwaltung/behoerden/behoerde-fuer-stadtentwicklung-und-wohnen/themen/wohnen/bauen/wege-zur-baugenehmigung/faqs/bauo-190372> (date of access: 03.05.2025).

²²⁰ Stadt Ulm. Digitale Stadt. URL: <https://www.ulm.de/leben-in-ulm/digitale-stadt> (date of access: 03.05.2025).

Таким чином, локальні статuti в містах Німеччини ефективно доповнюють регіональні стратегічні документи щодо цифровізації, тим самим створюючи дієві нормативно-правові механізми для реалізації ідей та принципів Smart City.

У своїй сукупності усі ці документи формують цілісний правовий каркас для впровадження та розвитку розумних міст у Німеччині та забезпечують їх узгодженість з європейськими стандартами. При цьому очевидно, що регламентація концепції «Smart City» у ФРН характеризується принципом «субсидіарності», де власне Федерація формує загальні цілі, а також активно підтримує фінансово й науково-дослідними ресурсами. Землі деталізують ці цілі у власних стратегіях та нормативних актах. А муніципалітети, у свою чергу, конкретизують і практично реалізують рішення з урахуванням місцевих потреб та особливостей громад. Це створює інтегровану, гнучку й водночас досить дієву систему, де кожен рівень має чітко визначену роль в управлінні «розумними» містами.

Отже, для ефективного розвитку smart-інфраструктури міста потрібна узгоджена та багаторівнева правова база, що охоплює як національні, так і муніципальні ініціативи.

З розвитком цифрового врядування, активною інтеграцією різноманітних технологій у публічно-управлінські процеси, а також зростанням суспільного запиту на прозорість, підзвітність і кібербезпеку, дедалі актуальнішою стає потреба у виокремленні муніципального інституційно-правового виміру концепції Smart City в українських реаліях. *Перш за все, це означає:*

- формування правових засад для стратегічного цифрового планування на муніципальному рівні, включно з розробкою, реалізацією та моніторингом міських цифрових стратегій, програм та планів цифрової трансформації міст, що відповідають принципам сталості (збалансованості);
- створення правової основи для врегулювання питань щодо ефективної реалізації муніципальної влади в процесі використання ІКТ, відкритих даних, smart-інфраструктури;

- визначення муніципально-правового статусу міських цифрових сервісів, штучного інтелекту, автономного міського транспорту, міських цифрових платформ;
- охорона та захист цифрових прав мешканців міст та громад, зокрема щодо приватності, участі, безпеки;
- забезпечення в межах міста правової інклюзії, тобто доступності цифрових сервісів для вразливих груп населення (люди з інвалідністю, маломобільні особи, літні люди тощо);
- запровадження правових механізмів екологічної відповідальності, що забезпечують сталий міський розвиток через цифрові інструменти (наприклад, енергомоніторинг, smart-grid (розумна мережа), управління викидами);
- закріплення цифрового суверенітету міст, зокрема права громади на управління власними міськими даними та цифровою інфраструктурою;
- необхідність підвищення цифрової кваліфікації муніципальних службовців як передумови ефективного та етичного використання цифрових інструментів управління, аналітики та комунікації;
- правове забезпечення розвитку так званої «цифрової просвіти», тобто обов'язок муніципалітетів розвивати цифрову компетентність жителів міст, з особливим акцентом на здатність реалізовувати цифрові права, користуватися електронними сервісами та брати участь у міському врядуванні;
- розвиток міжмуніципальної цифрової співпраці, зокрема через формування юридичних механізмів для врегулювання питань щодо створення спільних цифрових платформ, обміну відкритими даними, уніфікації стандартів Smart City, а також спільного впровадження інноваційних рішень у сферах міського управління, міської мобільності, сталого міського розвитку та кібербезпеки;
- створення правових умов для експериментування та інновацій, зокрема через «регуляторні пісочниці» (regulatory sandboxes), які дозволяють тестувати smart-рішення без порушення законодавства.

Таким чином правовий вимір концепту «розумного» міста слід розглядати як невід’ємну частину правового забезпечення балансу між впровадженням у містах інноваційних цифрових рішень і захистом публічних інтересів, муніципальних прав і свобод людини і громадянина.

Його роль особливо важлива у таких аспектах:

- Нормативно-правове регулювання цифрової трансформації міст: впровадження відкритих даних, електронної ідентифікації, кібербезпеки, обробки персональних даних, інструментів електронного урядування тощо потребує стабільної й передбачуваної юридичної бази.
- Закріплення механізмів цифрової участі: інститути партиципативного бюджету, громадських слухань, електронних петицій та місцевих ініціатив мають бути не лише технічно доступними, але й юридично гарантованими.
- Гарантії цифрових прав мешканців: у розумному місті цифрова інклюзія, доступ до інформації, право на захист персональних даних та алгоритмічну справедливість стають новими формами правових гарантій.
- Регулювання використання технологій штучного інтелекту: правова оцінка рішень, що приймаються автоматизовано, відповідальність за помилки алгоритмів, прозорість логіки їх роботи – усе це сфери, що потребують належного правового супроводу.

Отже, муніципально-правовий вимір Smart City має всі підстави розглядатися як окрема, рівнозначна складова поряд із технологічним, соціальним, екологічним, економічним та інституційним аспектами. Адже його ігнорування або недооцінка здатні поставити під загрозу цілісність впровадження концепції Smart City, її легітимність, ефективність та довгострокову сталість.

4. Значення Smart City для студентів-юристів

Для майбутніх правників ознайомлення з концепцією «розумного» міста має високу міждисциплінарну та практичну цінність. По-перше, ця тематика демонструє, як сучасні технологічні тренди впливають на право – від міжнародного рівня до муніципального. Студенти-юристи, вивчаючи ідеї та принципи *Smart City*, особливості функціонування smart-інфраструктури, набувають розуміння того, як право реагує на інновації, адаптуючи класичні правові інститути (наприклад, приватність, публічні послуги, демократичні процедури) до цифрової епохи. Це сприяє розвитку мислення, необхідного для роботи в умовах стрімких змін – вміння аналізувати нові ситуації, яких не знало традиційне право, і знаходити правильні та ефективні юридичні рішення для них.

По-друге, *Smart City* є яскравим прикладом міжгалузевого явища: воно лежить на перетині муніципального права, ІТ-права, адміністративного права, права інтелектуальної власності, екологічного права та навіть конституційного права (коли мова йде про права людини). Така комплексність дає майбутнім юристам нагоду бачити ширший контекст застосування положень та норм, а також взаємозв'язок складових елементів системи права. Зокрема, розуміння принципів обробки даних і кібербезпеки буде корисним навіть тим, хто спеціалізується у публічному праві, адже міста дедалі більше залежать від ІТ-систем і юристу міської ради потрібно розуміти базові технічні терміни та ризики.

По-третє, знання про *Smart City* має практичну корисність для професійної підготовки юристів, які планують працювати як у державному секторі, так і в приватному. В органах місцевого самоврядування зростає запит на фахівців, здатних розробляти регуляції для смарт-рішень, оцінювати юридичні наслідки впровадження нових технологій (наприклад, аналіз відповідності проєкту «розумного» відеоспостереження вимогам законодавства про захист даних), укладати складні договори державно-приватного партнерства, спрямовані на

розбудову міської IT-інфраструктури. У приватному секторі – компаніям, що розробляють рішення для «розумних» міст або консультують представників муніципальної влади, також потрібні юристи, обізнані як у праві, так і в технологіях. Такі юристи можуть займатися питаннями ліцензування програмного забезпечення для міста, захисту патентів на технології Smart City, відповідності продуктів вимогам безпеки та стандартам, судовими спорами щодо відповідальності за збої смарт-систем тощо.

Окрім того, *Smart City* ставить перед юристами нові етичні й філософські питання, які важливо усвідомлювати ще під час навчання. Наприклад: Як збалансувати цифрові інновації та права людини? Де межа між законним спостереженням заради безпеки і порушенням приватності? Як гарантувати недискримінаційність алгоритмів, які використовує публічна влада (щоб, скажімо, система «розумного» розподілу ресурсів не упереджувала якусь групу населення)? Такі питання виходять за рамки виключно технічних і очевидно потребують глибокого розуміння принципів верховенства права, юридичної відповідальності та соціальної справедливості. Розглядаючи їх на прикладі концепту *Smart City*, студенти-юристи вчаться формулювати правові підходи до вирішення нових викликів цифрової епохи. Адже рух до *Smart City* зрештою вимагатиме структурних змін у локальному врядуванні, а також оновленні нормативно-правових основ діяльності муніципалітетів.

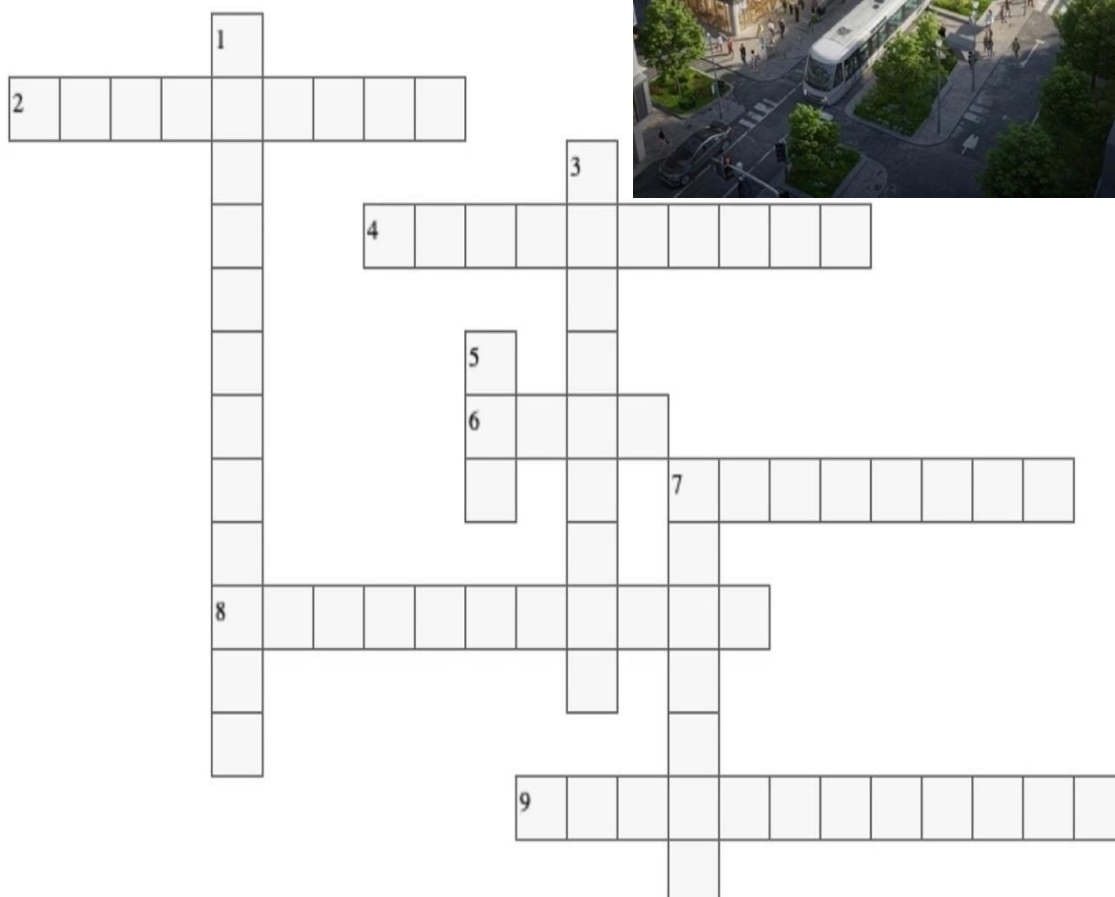
Отже, саме нинішнім студентам випаде завдання в майбутньому модернізувати правову систему міст – створити такі норми і механізми, що дозволять повною мірою реалізувати потенціал «розумних» технологій на благо громади, не поступаючись при цьому фундаментальними правами і цінностями суспільства. Знання концепції *Smart City* дає майбутнім правникам ключ до розуміння цих процесів і готує їх бути компетентними учасниками формування цифрового майбутнього міст.

Smart City – це багатовимірна концепція, що пройшла шлях від маркетингової категорії до важливого напрямку муніципальної політики та права. Сучасне «розумне» місто – це не лише про технології, але й про нові

моделі врядування, активну участь жителів у вирішенні питань місцевого значення, а також досягнення на місцевому рівні цілей сталого розвитку. Озброєні ґрунтовними знаннями, юристи можуть забезпечити те, щоб концепт Smart City всебічно реалізовувався як дійсно «розумне» – тобто юридично обґрунтоване та врегульоване, орієнтоване на людину, технологічно прогресивне та соціально відповідальне урбаністичне середовище.

ПЕРЕВІРКА ЗНАНЬ

Для закріплення пройденого матеріалу розв'яжіть кросворд.



По горизонталі

2. Прізвище керівника групи європейських дослідників, які першими у 2007 році опублікували рейтинг «Розумні міста – рейтинг середніх міст Європи».
4. Ключова ознака Smart City, що виражається в здатності міста використовувати дані, цифрові технології та інновації для сталого розвитку й підвищення якості життя.
6. Прізвище американського урбаніста, який описав три хвилі еволюції «розумних» міст.
7. Критерій розвитку міст, що передбачає баланс між економікою, екологією та соціальною сферою
8. Цифрова форма здійснення публічного управління, що передбачає використання ІКТ для надання публічних послуг, прозорості та участі громадян.
9. Процес впровадження цифрових технологій у всі сфери суспільного життя та управління.

По вертикалі

1. Стан захищеності кіберпростору, за якого забезпечується стійке функціонування, цілісність і конфіденційність інформації, що обробляється в ньому, а також безперервний доступ до неї в інтересах фізичних та юридичних осіб, суспільства і держави.
3. Перше місто, в якому у 1994 році було створено віртуальне «цифрове місто» як експеримент в галузі Smart City.
5. Аббревіатура для позначення цифрових технологій, що забезпечують обмін інформацією та зв'язок.
7. Пристрої Інтернету речей, які фіксують показники трафіку, освітлення, забруднення повітря тощо.

ЗАВДАННЯ

**1. Legal opinion for a municipal authority**

Міська рада планує впровадити систему відеоспостереження з елементами розпізнавання облич у рамках Smart City.

Підготуйте юридичний висновок про правомірність такої ініціативи з урахуванням права на приватність, GDPR, положень Конституції України та Закону України «Про захист персональних даних».

**2. Model Debate «The Digital City – Threat or Opportunity?»**

Поділіться на дві команди:

- 1: Захисники ідеї Smart City (ефективність, прозорість, екологічність тощо);
- 2: Критики (ризики цифрової дискримінації, втручання в приватність, кіберзагрози тощо).

Підготуйте аргументи на основі реальних кейсів, враховуючи відповідний досвід міст ЄС.



3. Comparative Legal Study: Smart City in Ukraine and Germany

Порівняйте правові механізми регулювання Smart City у місті Київ та місті Гамбург (або іншому німецькому місті).

Key criteria:

- *Наявність концепції Smart City;*
- *Регулювання кібербезпеки;*
- *Громадська участь;*
- *Доступ до відкритих даних.*

Представте результати у вигляді інфографіки або короткої презентації (5–7 слайдів).

Розділ XIII ПРАВОВІ ОСНОВИ КІБЕРБЕЗПЕКИ

LEGAL BASIS OF CYBERSECURITY

1. Визначення поняття кібербезпеки

У сучасному світі, де інформаційні та комунікаційні технології стали основою економічного, соціального та політичного розвитку, проблема кібербезпеки є надзвичайно важливою. Цифровізація майже всіх сфер діяльності приносить не лише нові можливості, але й нові ризики. Кіберзлочинність (cybercrime), зокрема кібератаки на критичну інфраструктуру, інтернет-шахрайство, а також незаконний доступ до персональних даних і фінансових ресурсів, ставлять під загрозу стабільність світових економік, безпеку держав і захист прав людини.



Зі зростанням обсягів цифрових даних, активним використанням інтернету для фінансових, управлінських і комунікаційних операцій, а також розвитком таких новітніх технологій, як штучний інтелект і блокчейн, виникає необхідність у створенні ефективної правової бази для захисту інформаційних ресурсів. Кібербезпека вже не обмежується лише технічними аспектами, а стала комплексною проблемою, що охоплює правові, організаційні, соціальні та економічні питання. Оскільки кіберзагрози порушують не лише безпеку даних, але й ставлять під сумнів функціонування критичних інфраструктур, важливо розробити ефективні правові механізми, які забезпечать їх захист.

Актуальність проблеми кібербезпеки полягає в тому, що на сьогоднішній день правове регулювання цієї сфери часто не відповідає швидким змінам технологічних загроз. Законодавство багатьох країн, зокрема й України, потребує оновлення для належної реакції на новітні виклики, пов'язані з кіберзлочинністю, захистом персональних даних та забезпеченням безпеки в умовах цифровізації. У цьому контексті важливим є не тільки вдосконалення

національних норм, але й інтеграція міжнародних стандартів та співпраця з іншими державами для ефективної боротьби з кіберзагрозами.



Кібербезпека є складною і багатогранною категорією, що охоплює систему заходів для захисту інформаційних ресурсів, систем, мереж та даних від різноманітних загроз, таких як несанкціонований

доступ, модифікація, пошкодження або знищення інформації. Вона включає захист комп'ютерних систем і мереж від атак, а також забезпечення конфіденційності та правильності оброблених даних. Кібербезпека є важливою складовою частиною національної безпеки та глобальної економічної стабільності, оскільки її ефективний захист дозволяє уникнути значних фінансових, політичних і соціальних наслідків.

В Законі України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року остання визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі²²¹.

Основними складовими кібербезпеки можна визначити: 1) *захист інформаційних систем і мереж*, шляхом використання технічних та організаційних засобів для забезпечення безпеки даних, що зберігаються або обробляються; 2) *захист персональних даних*, або забезпечення конфіденційності та безпеки персональних даних, а також контроль за їх використанням відповідно до норм права; 3) *запобігання кіберзлочинності*, правове регулювання та протидія кіберзлочинам, таким як крадіжка даних,

²²¹ Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 28.04.2025).

кібершахрайство, атаки на критичну інфраструктуру; 4) *реагування на інциденти кібербезпеки*, заходи, що включають виявлення, аналіз і ліквідацію наслідків кіберзагроз.

Таким чином, кібербезпека є не лише технічним, а й правовим феноменом, що вимагає чіткої правової основи для забезпечення безпеки цифрових систем, захисту прав користувачів інтернету та боротьби з кіберзлочинністю на національному і міжнародному рівнях.

2. Правове регулювання кібербезпеки

На сьогодні правове підґрунтя кібербезпеки України становлять міжнародні та національні нормативно-правові акти, які регулюють захист інформаційних ресурсів, мереж і систем від кіберзагроз, а також визначають відповідальність за порушення в цій сфері. Включає як загальні принципи кібербезпеки, так і детальні норми, що стосуються боротьби з кіберзлочинністю, захисту персональних даних і забезпечення безпеки критичних інфраструктур.

Серед міжнародних нормативно-правових актів можна зазначити, перш за все, Конвенцію Ради Європи про кіберзлочинність (Будапештська конвенція, 2001). Будапештська конвенція є першим міжнародним документом, що встановлює стандарти для боротьби з кіберзлочинністю на глобальному рівні. Вона визначає криміналізацію таких кіберзлочинів, як несанкціоноване втручання в комп'ютерні системи, поширення шкідливого програмного забезпечення, а також встановлює механізми співпраці між державами для боротьби з кіберзлочинами. Україна є учасником цієї конвенції, що дозволяє інтегрувати міжнародні стандарти в національне законодавство²²².

Окрім Будапештської конвенції слід згадати і про Рекомендації Організації Об'єднаних Націй (далі – ООН) щодо кібербезпеки²²³. ООН

²²² Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001: станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 28.04.2025).

²²³ Резолюція Генеральної Асамблеї ООН 70/237 (2015) «Розвиток інтернету та кібербезпеки». URL: <https://undocs.org/A/RES/70/237> (дата звернення: 28.04.2025).

розробила низку рекомендацій, спрямованих на зміцнення кібербезпеки в глобальному масштабі. Ці рекомендації охоплюють боротьбу з кіберзлочинністю, захист інфраструктури, захист прав людини в цифровому середовищі та забезпечення міжнародної співпраці для протидії глобальним кіберзагрозам. Вони стали основою для багатьох національних і міжнародних стратегій кібербезпеки ²²⁴.

Серед національних нормативно-правових актів доречно вказати: Конституція України²²⁵; Кримінальний кодекс України²²⁶, правові норми якого забезпечують правову основу для боротьби з кіберзлочинністю та захисту кіберпростору, а також встановлюють санкції за порушення безпеки інформаційних систем; ЗУ «Про основні засади забезпечення кібербезпеки України»²²⁷, який визначає основні принципи і механізми для забезпечення кібербезпеки в Україні, закріплюючи правову основу для захисту інформаційних систем, інфраструктур та даних від кіберзагроз; ЗУ «Про захист персональних даних»²²⁸, який регулює питання захисту персональних даних, що є важливою складовою кібербезпеки, зобов'язує організації, які збирають і обробляють персональні дані, вживати заходів для їх захисту від несанкціонованого доступу, а також створює правову основу для захисту приватності громадян у цифровому середовищі та інші.

3. Ключові загрози та властивості кібербезпеки

Враховуючи постійний розвиток інформаційних технологій, кіберпростір стає все більш вразливим до різноманітних загроз. Основні з них включають:

²²⁴ Резолюція Генеральної Асамблеї ООН 73/27 (2018) «Глобальна кібербезпека». URL: <https://undocs.org/A/RES/73/27> (дата звернення: 28.04.2025).

²²⁵ Конституція України : Прийнята на п'ятій сесії Верхов. Ради України 28 черв. 1996 р.. Донецьк : Сталкер, 2004. 64 с.

²²⁶ Кримінальний кодекс України : Офіц. вид.: Текст прийнятий Верхов. Радою України 5 квіт. 2001 р. Зі змін. та допов. станом на 1 квіт. 2004 р. Київ : ІнЮре, 2004. 240 с.

²²⁷ Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 28.04.2025).

²²⁸ Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 28.04.2025).



Hacker experience
But I must explain to you how all this mistaken idea
of denouncing pleasure and praising pain was born

✓ **Кібератаки** (cyberattack). Це одна із

найбільших загроз для безпеки в кіберпросторі, оскільки вони можуть мати руйнівний ефект як для окремих користувачів, так і для організацій або навіть цілих держав. Кібератаки мають різні форми, в залежності від цілей зловмисників і технологій, які ними використовуються. Вони

включають: 1) *DDoS-атаки* - атаки типу відмови в обслуговуванні, які направлені на перевантаження ресурсу (вебсайту, сервера або мережі) величезною кількістю запитів. Зловмисники можуть використовувати розподілені мережі комп'ютерів для створення величезного навантаження на цільову систему, що призводить до її виходу з ладу або значної деградації продуктивності. Це може мати катастрофічні наслідки для організацій, що залежать від онлайн-ресурсів для ведення бізнесу, включаючи фінансові втрати та репутаційні ризики; 2) *SQL-ін'єкції*, що є одним з найпоширеніших методів кібератак, спрямованих на вразливість веб-застосунків, які використовують бази даних SQL. Зловмисники вводять шкідливі SQL-запити в поля введення даних на веб-сайті, що дозволяє їм отримувати доступ до конфіденційної інформації, змінювати бази даних або навіть видаляти їх. Невірні налаштування безпеки в базах даних і недостатній рівень перевірки введених даних можуть дозволити зловмисникам здійснити такі атаки.

✓ **Віруси та шкідливе програмне**

забезпечення, до якого відносяться віруси, трояни, хробаки, шпигунські програми та інші види шкідливих кодів, та є одним із основних інструментів кіберзлочинців для здійснення несанкціонованих атак на інформаційні системи. Це програмне забезпечення може бути використане для досягнення наступних



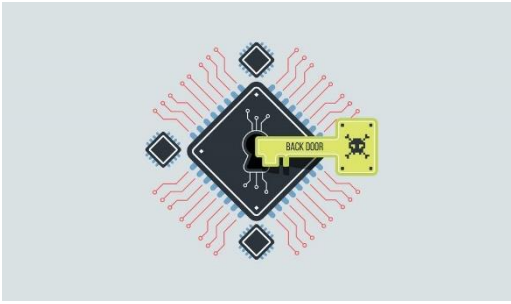
цілей. *Викрадення особистих даних і логінів користувачів.* Шкідливі програми, зокрема трояни і клавіатурні шпіони, можуть без відома користувачів збирати їх

персональні дані, логіни, паролі, а також інформацію про платіжні картки або інші чутливі дані, які пізніше можуть бути використані зловмисниками для здійснення фінансових злочинів. *Пошкодження або блокування даних.* Віруси, такі як програмне забезпечення-вимагач (ransomware), можуть зашифрувати дані на комп'ютері або в мережі і вимагати викуп за їх розшифровку. Крім того, віруси можуть знищувати важливі дані або заражати системи таким чином, що відновити їх неможливо. *Зниження продуктивності системи.* Шкідливі програми можуть споживати значну кількість системних ресурсів, що веде до зниження продуктивності комп'ютерів або серверів, внаслідок чого організації можуть зазнати фінансових втрат через зупинення роботи чи зниження ефективності.



✓ **Фішинг (phishing)** - одна з найбільш поширених технік соціальної інженерії, яку використовують кіберзлочинці для отримання конфіденційної інформації від користувачів через створення фальшивих вебсайтів або розсилку

підроблених електронних листів. Зловмисники можуть вдаватися до таких методів. *Підробка електронних листів.* Користувач отримує лист, який виглядає так, ніби він надісланий від банку, популярного онлайн-магазину або іншої організації, і містить посилання на підроблений вебсайт, де користувач має ввести свої особисті дані. Цей процес часто відбувається під виглядом перевірки безпеки або оновлення профілю. *Підробка вебсайтів.* Шахраї можуть створювати фальшиві вебсайти, схожі на офіційні сайти банків, електронної пошти або платіжних систем. Ці сайти використовуються для збору даних користувачів, які згодом можуть бути використані для незаконних фінансових операцій. Фішинг є надзвичайно ефективним методом, оскільки він експлуатує людський фактор, використовуючи наївність користувачів для збору цінних даних.



Вразливості

сучасних

інформаційних систем. Сучасні інформаційні системи, навіть з високим рівнем технічного захисту, можуть мати вразливості, які роблять їх об'єктами для кібернападів. До основних

вразливостей можна віднести. *Низький рівень безпеки програмного забезпечення.* Недостатнє тестування програмного забезпечення на наявність вразливостей або використання старих версій програм, які більше не підтримуються, може залишати відкритими двері для атак. *Невірні налаштування апаратного забезпечення та програмних систем.* Часто компанії або користувачі не налаштовують свої системи належним чином, що може призвести до ненавмисного відкриття доступу до конфіденційних даних. Наприклад, неактуальні паролі або неправильна конфігурація серверів можуть стати причиною несанкціонованого доступу. *Слабкий контроль доступу та недостатня політика захисту даних.* Відсутність чітких політик щодо доступу до чутливої інформації, слабкі або відсутні механізми автентифікації та авторизації, а також недостатня освіта персоналу можуть призвести до того, що організація стане жертвою кіберзлочинців, які скористаються цією слабкістю для вчинення злочинів.

4. Кіберзлочинність : визначення, типи та методи боротьби

Кіберзлочинність — це злочинна діяльність, яка здійснюється за допомогою інформаційно-комунікаційних технологій (далі - ІКТ), зокрема через Інтернет. Вона включає різноманітні протиправні дії, спрямовані на порушення прав та інтересів користувачів Інтернету, організацій, а також на шкоду державним інтересам в кіберпросторі. Кіберзлочинність може охоплювати широкий спектр злочинних діянь — від хакерських атак і крадіжки даних до фінансових шахрайств і кібертероризму.

Кіберзлочинність можна класифікувати за різними ознаками, зокрема за типами злочинних дій, які вчиняються. Основні види кіберзлочинів включають:

- ✓ **Кібершахрайство** - протиправні дії, спрямовані на обман або крадіжку грошей через Інтернет, зокрема через фішинг, підроблені онлайн-магазини, банківські шахрайства та інші види обману;
- ✓ **Крадіжка даних та персональної інформації** - злочини, пов'язані з несанкціонованим доступом до приватної інформації, зокрема персональних даних громадян, інтелектуальної власності компаній або державних установ;
- ✓ **Кібертероризм** - використання Інтернету та ІТ для здійснення терористичних актів або загроз, які спричиняють серйозні наслідки для суспільства, наприклад, атаки на критичну інфраструктуру або національні системи безпеки;
- ✓ **Атаки на критичну інфраструктуру** – «злам» комп'ютерних систем, які забезпечують функціонування важливих об'єктів, таких як енергетичні мережі, водопостачання, транспортні системи;
- ✓ **Шахрайство з криптовалютою** - використання технологій блокчейн для обману користувачів та крадіжки коштів, пов'язаних з криптовалютою.

Кіберзлочини, комп'ютерні злочини, злочини в інтернеті. Що каже адвокат?²²⁹ Ознайомитись з правовими наслідками таких дій та особливостями кваліфікації відповідно до КК України можна за наданим гіперпосиланням.

Протидія кіберзлочинності вимагає комплексного підходу, що включає:

- 1) *технічні засоби захисту*, або використання брандмауерів, антивірусних програм, систем виявлення та запобігання вторгненням, а також криптографічних методів для захисту даних;
- 2) *розслідування та цифрові докази* - спеціалізовані органи правоохоронних органів повинні мати інструменти для збору та аналізу цифрових доказів у випадку кіберзлочинів;
- 3) *міжнародна співпраця*, так як кіберзлочинність має транснаціональний характер, важливою

²²⁹ Кіберзлочини, комп'ютерні злочини, злочини в інтернеті. Що каже адвокат? *Legal IT Group*. URL: https://www.youtube.com/watch?v=A_lhO31HwxE (дата звернення: 18.05.2025).

складовою боротьби є співпраця між країнами для забезпечення правопорядку в глобальному масштабі; 4) *освітні програми та підвищення обізнаності* для запобігання кіберзлочинам, важливим є навчання користувачів, в тому числі через кампанії з підвищення обізнаності щодо безпеки в Інтернеті та захисту



особистих даних.

Проект з кібербезпеки BRAMA (БРАМА)

https://t.me/brama_channel

БРАМА - це синергія громадян, приватного та державного секторів у протидії дезінформації та незаконному контенту в інформаційному просторі.

Кіберзлочинці постійно адаптуються до нових технологій, що робить боротьбу з кіберзлочинністю дедалі складнішою. Нові загрози, такі як атаки на Інтернет речей (IoT) або використання штучного інтелекту для скоєння злочинів, потребують від правових систем швидкої реакції та гнучкості. Крім того, з розвитком анонімних технологій, таких як блокчейн, виникають нові виклики для правоохоронних органів у відстеженні злочинців.

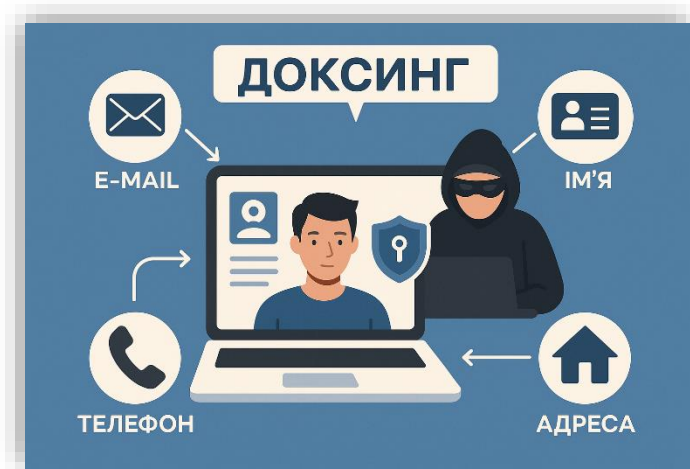


5. Доксинг

У сучасному цифровому світі, де значна частина нашого життя відбувається онлайн, зростає ризик розкриття особистої інформації без нашої згоди. Однією з таких загроз є доксинг (іноді зустрічається як «доксінг») — практика збору, публікації та розповсюдження приватної інформації про людину без її згоди, з метою завдання шкоди, залякування або створення незручностей²³⁰.

Сам термін «doxing» походить від англійського слова «documents» («документи»), що вказує на розкриття особистих даних, які часто зберігаються в різноманітних документах або онлайн-профілях. Доксинг набув особливої популярності в інтернет-середовищі, де конфіденційна інформація може миттєво поширюватися та використовуватися проти жертв з руйнівними наслідками.

Як працює доксинг?



Процес доксингу може включати збирання широкого спектру особистих даних жертви. Це може бути справжнє (повне) ім'я, домашня адреса, номер телефону, адреса електронної пошти, місце роботи, фінансові дані, особисті фотографії або будь-яка інша персональна інформація, яка

зазвичай не є публічною. У деяких, особливо агресивних випадках, зловмисники можуть навіть знаходити та оприлюднювати деталі про членів сім'ї жертви, розширюючи таким чином коло потенційної загрози.

Використовуючи зібрану інформацію, доксери можуть вдаватися до різних шкідливих дій. Це можуть бути прямі погрози фізичною розправою, шантаж з

²³⁰ Ковальчук А.Ю., Чернявська Б.В. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. Випуск 85: частина 4. 2024. С. 257-263.

вимогою певних дій, публічне дискредитування репутації жертви, розсилання спаму або навіть реальні дії, що наражають жертву на фізичну небезпеку чи незручності в реальному житті.

Прикладом наслідків доксингу є випадок, що стався у 2014 році під час конфлікту в спільноті геймерів під назвою «Gamergate». Кілька жінок, які відкрито виступали проти сексизму в індустрії відеоігор, стали жертвами скоординованих атак доксингу. Їхні особисті дані, включаючи домашні адреси та номери телефонів, були публічно оприлюднені в інтернеті, що призвело до отримання ними численних погроз насильством та інших форм онлайн-переслідування²³¹.

Інструменти та техніки доксингу

Зловмисники

використовують різноманітні інструменти та техніки для збору особистої інформації, серед яких найбільш поширеними є:

Такі платформи, як Facebook, Twitter, LinkedIn, Instagram та інші, є багатим джерелом особистої інформації. Доксери можуть ретельно аналізувати публікації, фотографії, інформацію в профілі, списки друзів та навіть геолокаційні мітки, щоб зібрати значний обсяг приватних даних про жертву.

Звичайний пошук в Google, Bing або інших пошукових системах може виявити велику кількість інформації,

ЗАХИСТ ВІД ДОКСИНГУ

Інструменти та техніки

-  **Соціальні мережі**
Обмежте доступ до інформації на Facebook, Twitter, LinkedIn та інших сайтах
-  **Пошукові системи**
Приберіть особисті дані, які були оприлюднені в Інтернеті раніше
-  **Злом облікових записів**
Захистіть акаунти за допомогою двофакторної автентифікації
-  **Бази даних та пошукові сайти**
Видаліть приватну інформацію з сайтів, що доступні через відкритий пошук
-  **Аналіз метаданих**
Вимикайте збереження геолокації в зображеннях

²³¹ Що таке доксинг (doxing, іноді – доксінг)? URL: <https://tseivo.com/b/jargoniist/t/pz1mjmyxqz/shcho-take-doksynh-doxing-inodi-doksinh#E-doksynh-vlasnykiv-erotychnoho-kontentu> (дата звернення: 30.04.2025).

особливо якщо жертва раніше публікувала її в інтернеті. Це можуть бути старі повідомлення на форумах, коментарі на новинних вебсайтах, записи в блогах або інші публічно доступні згадки.

Використання фішингових атак, підбору паролів або інших методів злому дозволяє доксерам отримати доступ до особистої електронної пошти або облікових записів у соціальних мережах жертви. Ці ресурси часто містять велику кількість конфіденційної інформації, включаючи приватні листування, особисті фотографії та контактні дані.

Існує ціла низка спеціалізованих вебсайтів, які займаються збором та агрегацією персональних даних. Деякі з них навіть пропонують платні послуги з пошуку інформації про людей за певними критеріями, такими як прізвище, номер телефону або адреса електронної пошти.

Метадані, що містяться у файлах зображень або документів, можуть випадково розкрити інформацію, яку користувач не мав наміру оприлюднювати.

Наприклад, географічні координати місця зйомки фотографії, дані про автора документа або час його створення.

Доксинг у криптосфері

Криптосфера, з її акцентом на анонімність та децентралізацію, здавалося б, повинна бути захищеною від розкриття особистої інформації. Проте, навіть у цій висококонфіденційній галузі випадки доксингу не є рідкістю і можуть мати особливо серйозні наслідки.



Наприклад, у 2014 році відомий розробник, який стояв за успішним криптовалютним проектом, став жертвою доксингу. Невідомому зловмиснику вдалося встановити справжнє ім'я розробника, його місце проживання та інші приватні дані. Ця інформація була опублікована в мережі, що призвело до отримання розробником погроз та створило значний ризик для його особистої

безпеки. Важливо зазначити, що в криптосфері розкриття анонімності ключових

осіб може не лише зашкодити їхній репутації, але й поставити під загрозу довіру та безпеку всієї платформи, над якою вони працюють²³².

Доксинг у криптосфері також несе значні ризики для звичайних користувачів. Зловмисники можуть використовувати отриману особисту інформацію для спроб отримання доступу до їхніх криптогаманців. Враховуючи незворотність криптовалютних транзакцій, успішна атака може призвести до значних фінансових втрат для жертви.

Однак варто зазначити, що інструменти доксингу можуть використовуватися і з протилежною метою. У випадках, коли анонімні криптовалютні проєкти виявляються шахрайськими та їхні розробники зникають з коштами інвесторів (так звані «rug pull»), спільнота розслідувачів може вдаватися до «зворотного доксингу». Метою таких дій є розкриття особистостей шахраїв для притягнення їх до відповідальності та спроби повернення вкрадених коштів інвесторів.

Хоча доксинг часто не передбачає незаконного збору інформації, його небезпека значно зростає через публічне розповсюдження. Об'єктом атаки є не лише приватність, але й фізична та психологічна безпека жертви, оскільки розкриття особистих даних може призвести до прямих погроз. Особливістю доксингу є його потенційний колективний вплив, коли оприлюднена інформація використовується для організації масованих онлайн-атак (тролінг, кібербулінг). Це зумовлює виділення доксингу в окремий делікт, оскільки він характеризується публічним розголошенням інформації без згоди особи з метою заподіяння шкоди, створення загрози та переслідування. Важливим є також право особи на забуття – можливість видалення шкідливої інформації про себе з загального доступу.

Міжнародно-правові аспекти протидії доксингу

Різні країни світу вживають законодавчих заходів для протидії доксингу, хоча підходи та нормативна база можуть відрізнятися.

²³² Що таке доксинг (doxing, іноді – доксінг)?. URL: <https://tseivo.com/b/jargoniist/t/pz1mjmyxqz/shcho-take-doksynh-doxing-inodi-doksinh#E-doksynh-vlasnykiv-erotychnoho-kontentu> (дата звернення: 30.04.2025).

У США правове регулювання доксингу фрагментоване та залежить від штату. Основу складають закони про кіберпереслідування, переслідування та погрози. Окремі штати, як Каліфорнія та Нью-Йорк, мають спеціальне законодавство, спрямоване на покарання за публікацію особистої інформації з метою залякування.

У Великобританії протидія доксингу здійснюється на основі «Закону про захист даних», який регулює обробку персональних даних та забороняє їх неправомірне розповсюдження, що може завдати шкоди. Також застосовується «Закон про шкідливі комунікації», що передбачає відповідальність за використання комунікацій (включно з електронними) для переслідування або залякування.

У Німеччині несанкціоноване розголошення особистих даних є кримінальним злочином згідно з Кримінальним кодексом та Загальним регламентом ЄС із захисту даних (GDPR). Доксинг може кваліфікуватися як кіберпереслідування, що також тягне за собою кримінальну відповідальність.

Кримінальний кодекс Франції встановлює відповідальність за незаконне розголошення приватної інформації, включаючи штрафи та тюремне ув'язнення.

У Австралії законодавство у сфері захисту персональних даних перебуває в процесі розвитку. Хоча спеціального закону про доксинг немає, судова практика та можлива кримінальна відповідальність за публікацію інформації з метою завдання шкоди є інструментами протидії. Також розглядаються ініціативи щодо розкриття даних анонімних інтернет-користувачів.

У Нідерландах з 2024 року введено окрему кримінальну відповідальність за доксинг до Кримінального кодексу. Доксинг визначається як дії, спрямовані на залякування, завдання серйозних незручностей або перешкоджання виконанню службових обов'язків шляхом розповсюдження персональних даних. За вчинення цього злочину передбачено покарання у вигляді позбавлення волі або штрафу, з посиленням відповідальності за доксинг проти певних категорій осіб²³³.

²³³ Ковальчук А.Ю., Чернявська Б.В. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. Випуск 85: частина 4. 2024. С. 257-263.

Корисні посилання:

1. <https://www.britannica.com/topic/doxing> - розкрито походження терміну, сучасні приклади та потенційні юридичні наслідки.
 2. <https://oercs.berkeley.edu/privacy/privacy-resources/protect-yourself-doxxing> - пояснюється, як захиститися від doxxing. Тут зібрані практичні поради: як мінімізувати цифровий слід, захистити свої облікові записи, виявити витoki даних та діяти у випадку doxxing-атаки. Це корисний гайд для кожного, хто хоче залишатися у безпеці в інтернеті.
 3. <https://sosafe-awareness.com/glossary/doxxing/> - можна дізнатися, як розпізнати, запобігти і захистити себе від цифрового переслідування.
-

ПЕРЕВІРКА ЗНАНЬ

What is true and what is false? Justify your answer.

1. Доксинг завжди передбачає незаконно отриману інформацію.
2. Термін «доксинг» походить від практики розкриття особистих даних, знайдених у «документах».
3. Право на забуття передбачає можливість особи видалити з інтернету будь-яку згадку про себе, навіть якщо ця інформація є правдивою та суспільно важливою.
4. У криптосфері анонімність завжди є абсолютним захистом від доксингу.
5. У криптосфері доксинг може лише зашкодити жертві та не має потенційних позитивних застосувань.
6. Фішинг — це метод технічного злому серверів компаній.
7. DDoS-атака направлена на перевантаження системи великою кількістю запитів.
8. Кібертероризм може включати атаки на енергомережі та водопостачання.

9. Програмне забезпечення-вимагач (ransomware) лише знищує дані.
10. Будапештська конвенція є першим міжнародним актом у сфері боротьби з кіберзлочинністю.

ЗАВДАННЯ



1. Legal Case Analysis

Знайдіть приклад гучної кібератаки або витоку персональних даних (наприклад, атака на енергомережу, витік у Facebook, злам банку тощо).

Describe:

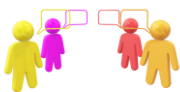
- хто був атакований;
- яка була мета;
- які наслідки;
- які заходи були вжиті (технічні й правові).



2. Legal comparative analysis

Порівняйте Закон України «Про основні засади забезпечення кібербезпеки» з подібним актом ЄС або США.

У чому основні відмінності? Які елементи міжнародного досвіду варто запровадити в Україні?



3. Practical Case Exercise «Cyberattack on a Government Body»

Roles: хакери, поліція, кіберспеціалісти, юристи, медіа.

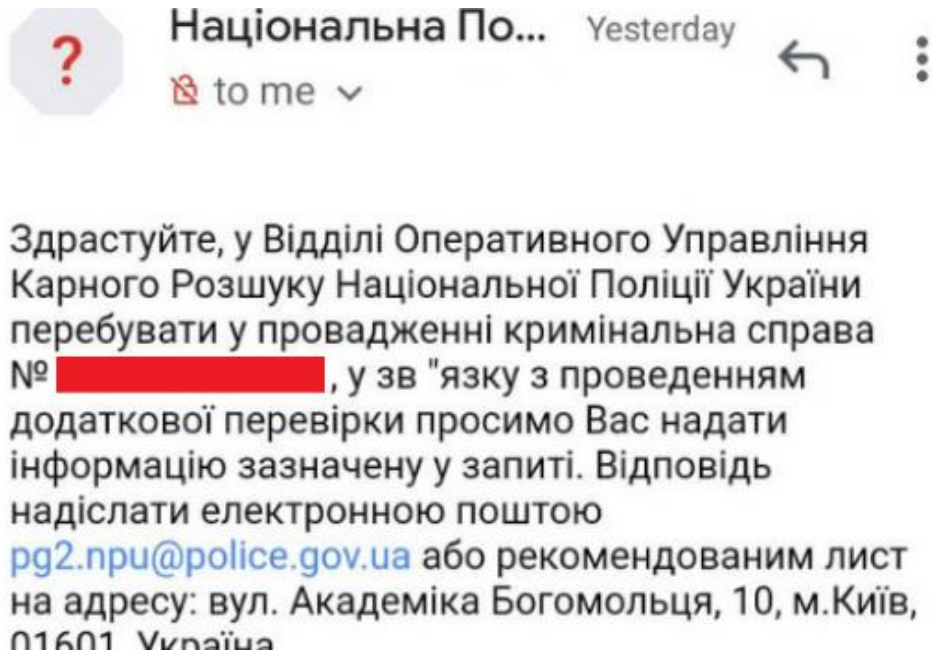
Scenario: на урядовий сайт здійснено DDoS-атаку.

Task: учасники мають відреагувати як команда кризового управління, запропонувати дії, пресреліз і правову оцінку.



4. Case study «Phishing Attack»

Детально проаналізуйте надані зразки листів та з'ясуйте чи є вони фішинговими.



Лабораторія цифрової безпеки

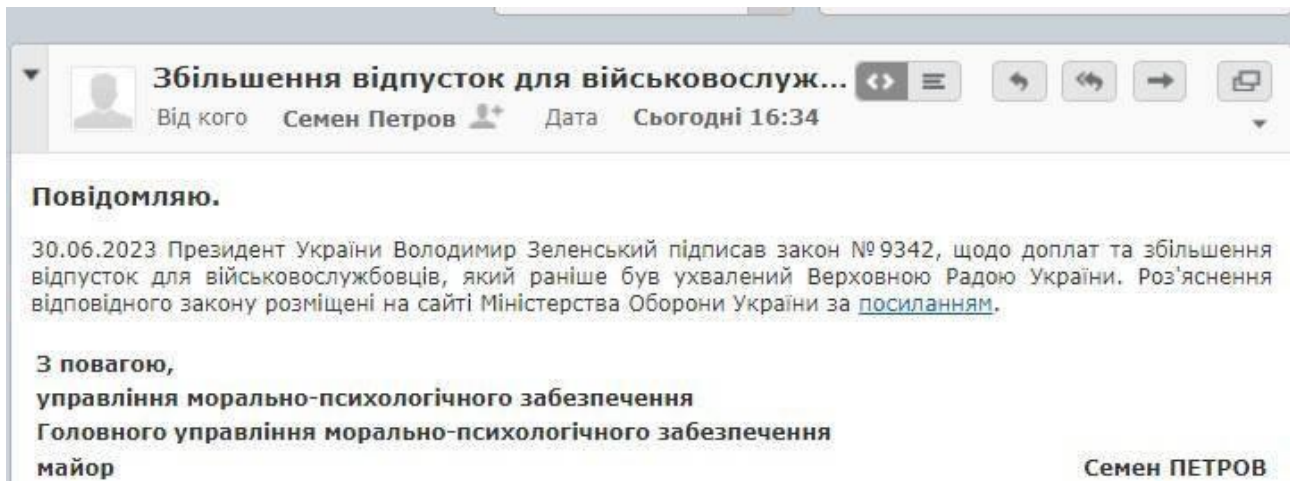


Фото: t.me/AFUStratCom



Ваш пакет відправляється

Планована дата доставки: субота, 19/06/2020

Це повідомлення надіслано, щоб повідомити, що ваш пакет оброблений для доставки. Клацніть посилання для відстеження нижче, щоб переглянути деталі доставки та перевірити фактичний стан транзиту вантажу.

[Клацніть, щоб переглянути деталі відправлення та номер відстеження.](#)

З щирою повагою

Нова Пошта

Московська, 46/2, Київ, Україна, 01001

Усі торговельні марки, торгові найменування або знаки обслуговування, що з'являються у зв'язку з «Новою Поштою», є власністю їх власників.

Скріншот CERT-UA

Ірина Кравчук



5. Debate «Should strong regulations be imposed on the use of cryptocurrencies?»

Команди «за» і «проти» мають підготувати аргументи з правової, технічної й етичної точки зору.



6. Case Study «Legal Responsibility for Cybercrime Fraud»

В Олега вкрали кошти через фішинговий сайт.

Questions:

- які статті Кримінального кодексу застосовуються;
- як би діяли правоохоронці;
- що повинен довести потерпілий у суді.

ПРЕДМЕТНИЙ ПОКАЖЧИК

- блокчейн, 31
- великі мовні моделі, LLM, 126
- віртуальні активи, 41
- генеративний ШІ, GenAI, 88
- декодерні моделі, 136
- доксинг, 240
- Дорожня карта з врегулювання штучного інтелекту в Україні, 100
- електронний кіднепінг, 22
- електронний суд, 189
- енкодерні моделі, 136
- ефект «чорної скриньки», 107
- Єдина судова інформаційно-телекомунікаційна система (ЄСІТС), 190
- інформаційна безпека, 157
- кібератака, 235
- кібербезпека, 232
- кіберпростір, 19
- кібертероризм, 238
- кібершахрайство, 238
- комп'ютерний зір, CV, 87
- криптовалюта, 47
- машинне навчання, ML, 87
- метавсесвіт, 18
- моделі з відкритим програмним кодом, 133
- невзаємозамінні токени, NFT 56
- обробка природної мови, NLP, 87
- платіжні токени, 50
- правова інформатика, 155
- правовий дизайн, 143
- пропрієтарні моделі, 134
- Регламент MiCAR, 64
- системи ШІ високого ризику, 95
- смарт-контракт, 71
- стейблкоїни, 50
- текстовий процесор, 163
- текстовий редактор, 162
- температура LLM, 129
- токени, 46
- токени активів, 53
- токенізатор, 128
- утилітарні токени, 52
- фішинг, 236
- хардфорк, 73
- хеш, 33
- хмарні технології, 160
- цифрова ідентифікація, 36
- цифрова ідентичність, 22
- цифровізація в праві, 16
- цифрова власність, 23
- шахрайство з криптовалютою, 238
- штучний інтелект, AI, 84
- Artificial Intelligence Act, 93
- LegalTech, 103
- NFT-колекції Bored Ape Yacht Club, 57
- prompt-інженерія, 131
- Smart City, 201

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Навчальне видання

ЦИФРОВІЗАЦІЯ В ПРАВІ

Підручник

За редакцією кандидата юридичних наук,

доцента С. Костенко

Роздруковано з оригінал-макету

Підп. до друку 28.05.2025 р.

Формат 60*84 1/16. Папір офс.

Гарнітура Times New Roman. Ум. друк. арк. 14,64.

Наклад пр. 100. Зам. №7

Поліський національний університет

Старий бульвар, 7, Житомир, 10008

Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи ДК №7381 від 13.07.2021 р.