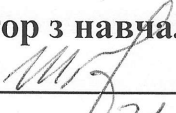


ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»
Факультет суспільних і прикладних наук
Кафедра права імені академіка УАН о. Івана Луцького

ЗАТВЕРДЖУЮ
Проректор з навчально-методичної роботи

_____ **Ярослав ШТАНЬКО**
«31» 08 2026 р.

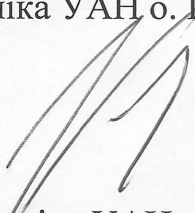
ІІІ В ПРАВНИЧІЙ ДІЯЛЬНОСТІ
силабус навчальної дисципліни

Галузь знань:	D Бізнес, адміністрування та право
Спеціальність:	D8 Право
Освітньо-професійна програма:	«Право»
Освітній рівень:	другий (магістерський)
Статус дисципліни:	обов'язкова
Мова викладання, навчання та оцінювання:	українська
Семестр викладання:	I

Івано-Франківськ
2026

РОЗРОБНИК:

Професор кафедри права імені академіка УАН о. Івана Луцького
доктор юридичних наук,
професор



Микола КАРЧЕВСЬКИЙ

ЗАТВЕРДЖЕНО:

на засіданні кафедри права імені академіка УАН о. Івана Луцького,
протокол № 1 від «28» серпня 2026 р.

В.о. завідувача кафедри
кандидат соціологічних наук,
доцент



Олександра ПТАШНИК

УЗГОДЖЕНО:

Гарант ОПП «Право»
доктор юридичних наук,
професор



Ірина БАСИСТА

СХВАЛЕНО:

на засіданні Науково-методичної ради,
протокол № 1 від «31» серпня 2026 р.

E-mail	mykola.karchevskyi@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра права імені академіка УАН о. Івана Луцького, ауд. 201
Сторінка курсу в СДО	ІІІ у професійній діяльності юриста (Moodle)

ВСТУП

Анотація навчальної дисципліни. Освітня компонента «ШІ в правничій діяльності»¹ призначена для підготовки магістрів права та формування у здобувачів вищої освіти системного розуміння технологій штучного інтелекту, їх можливостей, ризиків і правового регулювання. Курс поєднує технічні основи ШІ (машинне навчання, великі мовні моделі, генеративний ШІ) з практикою їх застосування в юридичній діяльності — від промпт-інжинірингу й аналізу документів до використання ШІ у державному управлінні, приватно-правових відносинах, кримінальній юстиції та LegalTech.

Особлива увага приділяється критичному й добросовісному використанню ШІ: розпізнаванню «галюцинацій» алгоритмів, алгоритмічній упередженості, проблемі «чорної скриньки», забезпеченню людського нагляду (human-in-the-loop), захисту персональних даних та адвокатської таємниці. Дисципліна ґрунтується на аналізі актуального законодавства (EU AI Act, GDPR, законодавство України) та ключових судових прецедентів (State v. Loomis, Schufa C-634/21, Mata v. Avianca, Thaler, справа Роберта Вільямса тощо).

Мета дисципліни та основні завдання: формування у здобувачів вищої освіти компетентностей із застосування технологій штучного інтелекту у професійній діяльності юриста на основі критичного аналізу можливостей і ризиків ШІ, розуміння правового регулювання ШІ та здатності приймати обґрунтовані рішення щодо добросовісного й безпечного використання відповідних інструментів.

Основними завданнями вивчення курсу є: опанування технічних основ і термінології ШІ; формування навичок промпт-інжинірингу та критичної оцінки згенерованих результатів; ознайомлення з підходами до правового регулювання ШІ в ЄС, США, Китаї та Україні; аналіз приватно-правових і кримінально-правових аспектів застосування ШІ; формування уявлення про перспективи розвитку LegalTech, квантових обчислень і технологій трансгуманізму та пов'язані з ними правові виклики.

У результаті вивчення дисципліни здобувач вищої освіти повинен **знати**:

- поняття, еволюцію та класифікацію технологій штучного інтелекту, принципи роботи великих мовних моделей та межі їхніх можливостей;

¹ У процесі роботи над силабусом було використано інструменти штучного інтелекту (Claude, ChatGPT, Gemini). ШІ застосовувалися для форматування та покращення тексту, пошуку джерел додаткової літератури й узагальнення практичних кейсів. Усі згенеровані за допомогою ШІ положення перевірено особисто розробником. Відповідальність за зміст силабусу несе розробник.

- переваги, технічні й когнітивні ризики використання ШІ в юридичній практиці та підходи до оцінки ефективності його впровадження;
- світові підходи до правового регулювання ШІ (EU AI Act, досвід США та Китаю) та стан регулювання ШІ в Україні;
- засади промпт-інжинірингу, методи аналізу документів і даних за допомогою ШІ, архітектуру RAG-систем;
- правові засади застосування ШІ у державному управлінні та електронному урядуванні, вимоги ст. 22 GDPR;
- приватно-правовий контекст ШІ: автоматизовані рішення, автоматизацію договірної роботи, авторське право та ШІ;
- кримінально-правові аспекти використання ШІ, застосування ШІ у діяльності правоохоронних органів і судів;
- тенденції розвитку LegalTech, правові виклики квантових обчислень і технологій трансгуманізму.

У результаті вивчення дисципліни здобувач вищої освіти повинен **вміти**:

- критично оцінювати можливості й обмеження інструментів ШІ під час вирішення юридичних завдань;
- застосовувати техніки промпт-інжинірингу (структурований промпт, анти-анкеринг, Chain-of-Thought, Chain-of-Verification, Few-Shot) та верифікувати згенеровані результати;
- кваліфікувати правові ситуації, пов'язані із застосуванням ШІ, з урахуванням EU AI Act, GDPR та законодавства України;
- виявляти технічні та когнітивні ризики використання ШІ (галюцинації, упередженість, дескілінг, планаризація) і пропонувати заходи їх мінімізації;
- розробляти локальні нормативні акти (політики, регламенти) щодо добросовісного та безпечного використання ШІ у професійній діяльності.

Компетентності та програмні результати навчання

Шифри та зміст компетентностей і програмних результатів навчання вказано відповідно до ОПП «Право» 2025 року для набору 2026 року.

Шифр та назва компетентності	Шифр та назва програмних результатів навчання
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.	ПРН 3. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та

	професійну літературу, бази даних, цифрові, сучасні методи дослідження.
ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	ПРН 4. Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.
СК6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію.	ПРН 8. Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.
СК9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності.	ПРН 9. Генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.
СК13. Здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією.	ПРН17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності

Зв'язок змісту освітньої компоненти з ПРН та компетентностями. Зміст курсу «ІІІ у професійній діяльності юриста» належним чином розкриває всі заявлені результати навчання та компетентності. Темі курсу охоплюють інтегрований аналіз, оцінку достовірності, використання технологій та правове регулювання ІІІ. Вони сприяють розвитку креативності, обґрунтуванню правових рішень та застосуванню сучасних правових доктрин у юридичній практиці.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	Перший	
Семестр	Перший	
Кількість кредитів ЄКТС	3 (90 год)	
Аудиторні навчальні заняття (денна форма):	Денна	Заочна
лекції	16	10
практичні (семінарські)	14	6
Самостійна робота	60 год	74
Форма підсумкового контролю	Екзамен	

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	Постреквізити
Професійна етика та дисциплінарна відповідальність правника	Практика ЄСПЛ у національній правовій системі
Ділова іноземна мова	Юридична практика
Верховенство права та правова система Європейського союзу	

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

Поняття та еволюція штучного інтелекту, його роль у сучасній трансформації юридичної практики та обґрунтування того, чому розуміння принципів роботи алгоритмів є обов'язковою компетенцією для сучасного правника. Значення цифрових компетентностей у контексті міжнародних орієнтирів, зокрема UNESCO AI Competency Framework for Students (AI CFS, 2024) та OECD Digital Education Outlook 2026, для формування професійного профілю студента-правника.

Тема 1. Основи технології штучного інтелекту. Що і чому необхідно знати юристу (2 год)

класифікація технологій: відмінності між машинним навчанням, глибоким навчанням та генеративним ШІ, а також принципи функціонування великих мовних моделей і межі їхніх технічних можливостей. Практичне застосування ШІ в юридичній діяльності, автоматизація рутинних завдань, аналіз судової практики та використання інструментів цифрової трансформації для оптимізації юридичної роботи.

Основні поняття: штучний інтелект, машинне навчання, генеративний ШІ, великі мовні моделі, юридичні технології, AI CFS 2024, OECD Digital Education Outlook 2026, компетенції ШІ.

Самостійна робота. У межах самостійної роботи опрацювати концепцію обов'язку технологічної компетентності (Duty of Technology Competency), проблему «чорної скриньки» та рамкові стандарти UNESCO AI CFS 2024 і OECD.

Тема 2. Переваги та ризики використання ШІ. Оцінка ефективності використання ШІ (2 год)

Критичний аналіз практичних переваг та потенційних ризиків застосування штучного інтелекту у юридичній практиці. Розгляд питань підвищення продуктивності, автоматизації рутинних завдань та оптимізації витрат.

Аналіз технічних та правових ризиків використання ШІ: феномен галюцинацій моделей, алгоритмічна упередженість (bias), проблема «чорної скриньки» (непояснюваність дій алгоритмів), проблема узгодження цілей та поведінки ШІ із людськими цінностями та правовими нормами (Alignment problem), порушення конфіденційності та витік персональних даних.

Вивчення когнітивних ризиків взаємодії юриста з інструментами ШІ: проблема планаризації (спрощення складного світу та правових контекстів),

епістемічна дистанція між юристом і джерелами знань, явище дескілінгу (втрата базових юридичних навичок аналізу та письмової аргументації). Дослідження ризиків введення даних (input problem), ефекту «якоріння» на первинних згенерованих варіантах, психологічної надмірної довіри до ШІ та проблеми перекладання професійної відповідальності на алгоритми. Визначення та оцінка метрик ефективності (ROI) впровадження інструментів ШІ в юридичних компаніях та оптимізація юридичного комплаєнсу.

Основні поняття: галюцинації ШІ, алгоритмічна упередженість, ефект «чорної скриньки», Alignment problem (проблема узгодження), конфіденційність, витік даних, когнітивні ризики, планаризація, епістемічна дистанція, дескілінг, input problem, ефект якоріння, надмірна довіра до ШІ, перекладання відповідальності, юридичний комплаєнс, оцінка ризиків, ROI у LegalTech.

Самостійна робота. У межах самостійної роботи розмежувати техніко-правові (галюцинації, Alignment problem, «чорна скринька») та когнітивні (дескілінг, епістемічна дистанція, ефект якоріння) ризики; ознайомитися з методологією оцінки ROI впровадження LegalTech.

Тема 3. Правове регулювання ШІ. Досвід ЄС, США та Китаю. Регулювання ШІ в Україні (2 год)

Світові підходи до нормативно-правового регулювання штучного інтелекту. Детальний аналіз Акту ЄС про штучний інтелект (EU AI Act) та застосування ризик-орієнтованого підходу, регуляторні ініціативи США (Executive Orders) та нормативні акти Китаю щодо генеративного ШІ. Вивчення Дорожньої карти з регулювання ШІ в Україні, адаптація українського законодавства до стандартів Європейського Союзу, використання інструментів м'якого (Soft Law) та жорсткого (Hard Law) права. Застосування регуляторних пісочниць (regulatory sandboxes) для апробації технологій ШІ та забезпечення прозорості алгоритмів. Основні поняття: EU AI Act, ризик-орієнтований підхід, Soft Law, Hard Law, регуляторні пісочниці, прозорість алгоритмів, Дорожня карта регулювання ШІ в Україні.

Самостійна робота. У межах самостійної роботи здійснити порівняння підходів ЄС (EU AI Act), США та Китаю, опрацювати Дорожню карту регулювання ШІ в Україні та механізм регуляторних пісочниць.

Тема 4. Генеративний ШІ та промпт-інжиніринг для юристів. Аналіз документів та даних за допомогою ШІ (2 год)

Практичні навички роботи з генеративним ШІ (ChatGPT, Claude, Copilot) та спеціалізованими юридичними сервісами. Застосування структурованої методики побудови юридичного промпту за схемою Персона → Контекст →

Проблема для первинного розбору показань свідків, документів та фактажу справи. Методи запобігання ефекту якоріння (анти-анкерінг) та формування власних гіпотез юриста перед зверненням до ШІ з формулюванням явних заборон у промпті.

Використання рольових інструкцій для залучення експертної логіки суміжних фахівців. Техніки декомпозиції промптів (Prompt Decomposition) для розбору складних аналітичних довідок та юридичних документів за блоками.

Застосування Few-Shot Prompting для уніфікації формату згенерованих матеріалів із суворим контролем недопущення домислювання фактів. Побудова покрокових міркувань із використанням Chain-of-Thought та алгоритму самоперевірки моделей Chain-of-Verification перед вирішальними процесуальними діями. Архітектура та принципи функціонування RAG-систем (Retrieval-Augmented Generation) для створення приватних юридичних баз знань, точного пошуку нормативних актів, підтягування релевантного контексту та мінімізації галюцинацій алгоритмів при роботі з великими масивами правової документації.

Методологія обробки юридичних даних та документації шляхом генерації та виконання коду (Python, SQL) за допомогою ШІ з метою автоматизованого парсингу, структурування, очищення та аналізу великих масивів неупорядкованих юридичних даних, реєстрів та судових рішень. Критична оцінка результатів генерації та усвідомлення трьох фундаментальних меж використання ШІ правником.

Трактування результатів ШІ як робочої чернетки, а не готової юридичної позиції чи доказу, із фіксацією параметрів запиту (інструмент, версія, промпт) для забезпечення прозорості методу. Подолання ефекту планаризації (стирання контексту та юридичних нюансів) шляхом застосування «тесту на спрощення» та свідомого відновлення багатовимірності правової картини. Управління епістемічною дистанцією між правником і джерелами знань та запобігання дескілінгу (втраті базових навичок юридичного аналізу та аргументації).

Основні поняття: генеративний ШІ, промпт-інжиніринг, юридичний промптинг, анти-анкерінг, Prompt Decomposition, Few-Shot Prompting, Chain-of-Thought, Chain-of-Verification, RAG (Retrieval-Augmented Generation), генерація коду ШІ, критична оцінка результатів, планаризація, епістемічна дистанція, дескілінг, тест на спрощення.

Самостійна робота. У межах самостійної роботи опанувати фреймворк «Персона → Контекст → Проблема», прийоми анти-анкерінгу, алгоритми Chain-of-Thought і Chain-of-Verification та засади роботи з RAG-системами.

Тема 5. Штучний інтелект у державному управлінні та електронному урядуванні (2 год)

Нормативна рамка алгоритмічного управління та детальний аналіз статті 22 GDPR: загальна заборона виключно автоматизованих рішень, три виключення (договір, закон, згода) та презумпція незаконності повної автоматизації в публічному секторі. Концепція «людини в контурі» (human-in-the-loop) та критерії відмежування змістовної участі людини від формального затвердження рішення алгоритмом.

Право на пояснення як передумова реалізації права на оскарження, вимоги до пояснення (проста форма, відносна вага факторів, своєчасність), концепція когнітивного суверенітету Л. Байгрейва та принцип алгоритмічної підзвітності.

Посилений захист вразливих груп (дітей, мігрантів, осіб з інвалідністю) та обов'язковість оцінки ризиків дискримінації. Визначення систем публічного управління як систем високого ризику за EU AI Act та дискусія навколо пакету Digital Omnibus (2025) у контексті конфлікту між дерегуляцією та захистом основоположних прав. Напрями використання ШІ за даними звіту OECD «Governing with Artificial Intelligence» (2025), співвідношення аналітичних завдань і рутинної автоматизації, проблема масштабування пілотних проєктів.

Вивчення кейсу MiDAS (Мічиган, справа Bauserman v. Michigan UIA) через призму автоматизованої несправедливості та принципу належної правової процедури (Due Process). Дослідження кейсу Amsterdam Smart Check, діагностичної функції ШІ щодо якості управлінського рішення та причин закриття проєкту. Практичне значення справи Schufa (C-634/21, Суд ЄС, 2023) щодо розширення поняття «рішення» у ст. 22(1) GDPR та унеможливлення обходу вимог через формальне збереження рішення за людиною.

ШІ у нормотворчості та формуванні публічної політики: підготовка проєктів, аналіз регуляторного впливу, опрацювання громадських консультацій, кейс Порту-Алегрі (2023) та проблема авторства норми. Виклики для демократичної легітимності в умовах алгоритмічного управління: епістемічна дистанція, дескілінг демократичних навичок та концепція алгократії (А. Фердман). Порівняльна характеристика двох вимірів застосування ШІ в публічному секторі (індивідуальні рішення щодо громадян проти нормотворчості) за їхніми профілями ризику та механізмами реагування.

Основні поняття: GDPR стаття 22, алгоритмічне врядування, human-in-the-loop, змістовний людський нагляд, право на пояснення, когнітивний суверенітет, EU AI Act, Digital Omnibus 2025, OECD Governing with AI, Due Process, кейс MiDAS, кейс Amsterdam Smart Check, справа Schufa, алгократія, алгоритмічна підзвітність, автоматизоване адміністративне рішення.

Самостійна робота. У межах самостійної роботи опрацювати ст. 22 GDPR і положення EU AI Act щодо систем високого ризику в публічному секторі, розмежування формального та змістовного людського нагляду й судову практику (Schufa, MiDAS).

Тема 6. Приватно-правовий контекст ШІ. Право не бути суб'єктом автоматизованих рішень. Автоматизація договірної роботи. Авторське право та ШІ (2 год)

Приватно-правовий вимір застосування штучного інтелекту та фундаментальні засади захисту приватного життя і персональних даних. Розгляд статті 22 GDPR як суб'єктивного права особи (суб'єкта даних) не підлягати рішенню, яке базується виключно на автоматизованій обробці, включаючи профайлінг, у відносинах між приватними суб'єктами (фінансовими установами, страховими компаніями, роботодавцями, цифровими платформами).

Проблема правосуб'єктності та юридичного статусу штучного інтелекту в цивільному праві. Дослідження концепцій «електронної особи» (electronic person), квазі-правосуб'єктності автономних систем, агентурної моделі та режиму джерела підвищеної небезпеки. Розподіл цивільно-правової відповідальності за шкоду, завдану діями або рішеннями штучного інтелекту між розробником, власником та користувачем. Автоматизація договірних відносин: співвідношення та конвергенція детермінованих смарт-контрактів (блокчейн-код за принципом «if-then») та інструментів штучного інтелекту.

Використання ШІ для аналізу, складання та аудиту угод, а також функціонування автономних ШІ-агентів у договірних процесах. Проблематика волевиявлення сторін, розподілу ризиків, помилок у коді та цивільно-правової відповідальності при автоматизованому укладенні та виконанні цифрових договорів. Проблеми права інтелектуальної власності в епоху розвитку ШІ. Дослідження правового режиму та специфіки авторського права на контент, згенерований штучним інтелектом (AI-generated content). Юридичні ризики та концепція добросовісного використання (Fair Use / Text and Data Mining) об'єктів інтелектуальної власності для навчання великих мовних моделей і нейромереж. Основні поняття: стаття 22 GDPR як право особи, профайлінг у приватному секторі, суб'єктність ШІ, електронна особа

(electronic person), цивільно-правова відповідальність ШІ, смарт-контракти, ШІ-агенти, автоматизоване укладення договорів, авторське право, AI-generated content, Text and Data Mining.

Самостійна робота. У межах самостійної роботи опрацювати межі застосування ст. 22 GDPR у приватних відносинах, доктрини цивільно-правової відповідальності за дії ШІ та правовий режим AI-generated content і Text and Data Mining.

Тема 7. ШІ та кримінально-правове регулювання. Використання ШІ для вчинення злочинів. ШІ в діяльності правоохоронних органів та судів (2 год)

Проблема «середньої людини» як методологічна рамка персоналізації правоохоронного впливу проти орієнтації на статистичний профіль «типового» злочинця. Напрями використання ШІ у поліцейській діяльності: оперативна підтримка, автоматизація рутини, дані звіту Police Foundation, застосування дронів із розпізнаванням обличчя та камери дорожнього руху з 4D-скануванням салону й ANPR. ШІ в кримінальному розслідуванні для опрацювання масивів цифрових доказів, аналізу слідів, транскрибування аудіо, виявлення прихованих мереж та апробація системи Soze (2024).

Превентивна діяльність, прогнозування попиту на послуги поліції та управління ризиками домашнього насильства. Просторовий рівень предиктивної поліцейської діяльності, логіка «гарячих точок», ефект «зворотної петлі» (feedback loop), дослідження HRDAG щодо PredPol та рішення Санта-Круз (2020). Індивідуальний рівень предикції на прикладі системи HART (Дарем), її архітектура, проблеми расових стереотипів у даних Experian та причини закриття у 2021 році. «Алгоритмічне усереднення» як правова проблема оцінювання особи за статистичною імовірністю поведінки групи замість вчиненого діяння у співвідношенні з принципами індивідуалізації відповідальності та презумпції невинуватості.

Правові наслідки біометричної ідентифікації та справа Роберта Вільямса (Детройт, 2020) з мировою угодою 2024 року як моделлю регулювання. Аналіз цифрових доказів платформою Longeye (2025) та мультимодальний аналіз записів боді-камер. Процесуальний статус алгоритмічно обробленого доказу, розмежування «інструменту пошуку» та власне доказу, проблеми «чорної скриньки» у контексті справ HART і Loomis. Стандарти допустимості алгоритмічних висновків у судочинстві, вимоги змістовного людського контролю, прозорості та відповідність гарантіям ст. 22 GDPR й EU AI Act.

Основні поняття: проблема «середньої людини», алгоритмічне усереднення, предиктивна поліцейська діяльність, PredPol, система HART, зворотно-петльовий ефект (feedback loop), розпізнавання облич, мирова угода Детройта 2024, платформа Longeye, справа Loomis, процесуальний статус алгоритмічного доказу, змістовний людський контроль, EU AI Act.

Самостійна робота. У межах самостійної роботи опрацювати співвідношення принципів індивідуалізації відповідальності та презумпції невинуватості з «алгоритмічним усередненням», стандарти допустимості цифрових доказів і ключові прецеденти (Loomis, справа Р. Вільямса).

Тема 8. Професійна юридична діяльність та розвиток технологій. LegalTech проекти на основі ШІ. Правове регулювання квантових обчислень та технологій трансгуманізму (2 год)

Майбутнє юридичної професії та ринок LegalTech проектів і стартапів на основі ШІ (Harvey, CoCounsel тощо). Правові наслідки розвитку квантових обчислень, загрози для постквантової криптографії та виклики трансгуманізму (нейротехнології, інтерфейси мозок-комп'ютер, захист нейроправ). Етичні стандарти та нові вимоги до адвокатської діяльності та професійної компетенції юристів в умовах технологічних трансформацій. Основні поняття: LegalTech, квантові обчислення, постквантова криптографія, трансгуманізм, нейроправа (neurorights), етика адвокатської діяльності, майбутнє юридичної професії.

Самостійна робота. У межах самостійної роботи опрацювати моделі трансформації юридичного бізнесу під впливом LegalTech (Harvey, CoCounsel), концепцію нейроправ і когнітивної свободи та правові виклики квантових обчислень.

Перелік тем семінарських занять

Семінар по темі 2(1). Переваги та ризики використання ШІ. Оцінка ефективності використання ШІ (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. 'Фантомний прецедент та витік даних': Аналіз технічних та етико-правових ризиків у судовій практиці

Адвокатське бюро «Право та Прогрес» здійснювало підготовку позовного заяви у складній корпоративній спорі. Молодший юрист, прагнучи прискорити роботу, використав публічну генеративну модель ШІ для пошуку релевантної судової практики та складання правової позиції. У процесуальний документ було завантажено вихідні фінансові документи клієнта та персональні дані керівників без попереднього знеособлення (input problem). Отриманий від ШІ текст містив посилання на п'ять рішень Верховної Ради/Верховного Суду з переконливими цитатами та номерами справ. Юрист, зазнавши «ефекту якоріння» на первинно згенерованому документі та маючи високий рівень психологічної довіри до алгоритму, не перевіряв наявність рішень у Єдиному державному реєстрі судових рішень (проблема епістемічної дистанції). У результаті під час судового засідання з'ясувалося, що три з п'яти наведених судових рішень є повністю згенерованими «галюцинаціями» ШІ, а конфіденційні дані клієнта потрапили до загальної бази навчання публічної моделі ШІ. Суд виніс окрему ухвалу щодо адвоката, а клієнт погрожує позовом через порушення конфіденційності.

Алгоритм обговорення:

Здійснити юридичну кваліфікацію дій юриста з точки зору Правил адвокатської етики, законодавства про захист персональних даних та процесуального права.

Диференціювати та проаналізувати проявлені у кейсі ризики: технічні (галюцинації, витік даних через input problem) та когнітивні (ефект якоріння, епістемічна дистанція, надмірна довіра).

Розробити покроковий алгоритм верифікації (Fact-Checking Framework) для перевірки юридичних текстів, згенерованих ШІ, перед їх поданням до суду.

Скласти проект Положення (SOP) юридичної компанії щодо безпечного використання інструментів штучного інтелекту та запобігання витоку конфіденційної інформації.

Критерії оцінювання:

Добре: Студент правильно ідентифікував юридичні порушення та ключові ризики (витік даних, вигадані судові рішення), однак аналіз когнітивних ризиків є неповним або поверхневим. Алгоритм верифікації містить загальні рекомендації без деталізації процедури перевірки джерел.

Відмінно: Студент надав вичерпну юридичну та методологічну оцінку ситуації, чітко розмежував технічні та когнітивні ризики, правильно застосував професійну термінологію (галюцинації, input problem, ефект якоріння, епістемічна дистанція). Запропоновано комплексний алгоритм верифікації та якісний проект локального нормативного акта щодо ШІ-комплаєнсу.

Задовільно: Студент обмежився описом факту фальсифікації судової практики та порушення конфіденційності без глибокого аналізу причин (когнітивних упереджень та особливостей функціонування LLM). Запропоновані кроки вирішення мають узагальнений декларативний характер.

Кейс 2. 'Оцінка ROI та ризику дескілінгу при впровадженні LegalTech в юридичному департаменті холдингу'

Керівник юридичного департаменту великого промислового холдингу подав генеральному директору запит на закупівлю та інтеграцію спеціалізованої LegalTech-платформи на базі ШІ для автоматизації перевірки та укладання типових договорів. Вартість впровадження системи становить \$50,000 на рік. За розрахунками розробника, система має скоротити час перевірки договорів на 70%, що дозволить скоротити штат молодших юристів або перенаправити їх на складніші завдання. Проте під час пілотного тестування виявилися наступні проблеми: 1) Молодші юристи перестали заглиблюватися в аналіз ризиків, сліпо погоджуючись із правками ШІ (виявлено ефекти дескілінгу та планаризації сприйняття юридичних контекстів); 2) Система показує алгоритмічну упередженість (bias) користь нестандартних формулювань, які відхиляють стандартні захисні застереження компанії; 3) Керівництво вимагає чіткого обґрунтування ROI (показника повернення інвестицій) з урахуванням потенційних збитків від юридичних помилок ШІ та витрат на комплаєнс.

Алгоритм обговорення:

Провести розрахунок метрик ефективності та ROI впровадження ШІ-інструменту (фінансові вигоди vs витрати на ліцензії, навчання та комплаєнс-контроль).

Проаналізувати когнітивні ризики (дескілінг, планаризація) та запропонувати програму підтримки та розвитку базових аналітичних навичок у молодших юристів в умовах автоматизації.

Оцінити правові та операційні ризики алгоритмічної упередженості (bias) та проблеми «чорної скриньки» при автоматизованому аналізі договорів.

Сформулювати матрицю юридичного комплаєнсу та контрольних точок (Human-in-the-loop), які мають бути обов'язковими при затвердженні договорів, опрацьованих ШІ.

Критерії оцінювання:

Добре: Розрахунок ROI виконано коректно, визначено основні ризики автоматизації договорів. Проте заходи щодо подолання дескілінгу та алгоритмічної упередженості є стандартними та недостатньо адаптованими до конкретної специфіки юридичної практики.

Відмінно: Проведено точний та різнобічний аналіз ROI з урахуванням як прямих економічних ефектів, так і ризик-адаптованих витрат. Глибоко розкрито сутність феноменів дескілінгу та планаризації, запропоновано дієву модель 'Human-in-the-loop' та програму збереження експертизи юристів.

Задовільно: Аналіз обмежений лише базовими фінансовими розрахунками без урахування юридичних та когнітивних ризиків. Проблема дескілінгу згадана формально, відсутні чіткі пропозиції щодо системи комплаєнсу та контролю рішень ШІ.

Рекомендації для самостійної роботи

Під час опрацювання теми зосередьте увагу на розмежуванні техніко-правових ризиків (феномен галюцинацій, Alignment problem, проблема «чорної скриньки») та когнітивних загроз для фахівця (дескілінг, епістемічна дистанція, ефект якоріння). Для комплексної оцінки доцільності впровадження LegalTech-інструментів опануйте методологію розрахунку ROI та алгоритми забезпечення юридичного комплаєнсу й захисту персональних даних при введенні запитів (input problem).

Питання для самоконтролю:

Як Alignment problem та ефект «чорної скриньки» (Black Box Problem) впливають на дотримання процесуальних гарантій та принципів рівності сторін при використанні ШІ у судочинстві?

У чому полягає сутність когнітивних ризиків дескілінгу та планаризації юридичного мислення при системному використанні генеративних моделей ШІ?

Які метрики (зокрема ROI) та комплаєнс-процедури є критичними для оцінки доцільності та безпечності впровадження інструментів LegalTech в юридичний департамент?

Завдання для самостійної роботи:

Розробіть проект внутрішнього регламенту (SOP) юридичної компанії щодо використання генеративного ШІ, врахувавши вимоги щодо запобігання витоку конфіденційних даних (input problem) та алгоритм перевірки судових прецедентів на предмет «галюцинацій».

Проведіть порівняльний аналіз ROI та сформулюйте матрицю ризиків (включно з ефектом якоріння та дескілінгом) для кейсу впровадження системи автоматизованого аналізу договорів (contract review) у корпоративній юридичній службі.

YouTube, онлайн-курси та корисні ресурси

Офіційний текст Регламенту ЄС про штучний інтелект (EU AI Act) на EUR-Lex - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Законодавство України на офіційному веб-порталі Верховної Ради України - <https://zakon.rada.gov.ua/>

Офіційний сайт Європейської ради з захисту даних (EDPB) - <https://edpb.europa.eu/>

Семінар по темі 3(2). Правове регулювання ШІ. Досвід ЄС, США та Китаю. Регулювання ШІ в Україні (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. HR-Tech стартап: Оцінка ризиків AI-системи рекрутингу за EU AI Act та правовий комплаєнс у регуляторній пісочниці України

Українська IT-компанія 'SmartHR Solutions' розробила мультимодальну систему штучного інтелекту 'TalentScan AI', призначену для автоматизації відбору кандидатів на вакансії. Система аналізує резюме, проводить автоматизоване первинне інтерв'ю (через аватар), використовує розпізнавання емоцій за виразом обличчя та тембром голосу для оцінки стресостійкості, а також здійснює автоматичне ранжування кандидатів за шкалою придатності. Компанія планує вийти на ринок ЄС (Німеччина, Франція), продавати рішення юридичним особам у США та одночасно протестувати сервіс в Україні в межах Дорожньої карти з регулювання ШІ, розробленої Міністерством цифрової трансформації. Компанії необхідно провести юридичний аудит продуктів, визначити рівні ризику, підготувати систему до вимог прозорості та розробити дорожню карту вступу до української регуляторної пісочниці (Regulatory Sandbox).

Алгоритм обговорення:

1. Кваліфікація та класифікація ризику за EU AI Act: провести юридичний аналіз функціоналу 'TalentScan AI' згідно з Додатком III до EU AI Act (визначення віднесення до системи високого ризику / High-Risk AI System через використання в сфері HR та доступу до працевлаштування) та ідентифікація заборонених практик (Unacceptable Risk) щодо аналізу емоцій на робочому місці/навчанні.
2. Порівняльно-правовий аналіз вимог у США та Китаї: оцінити відповідність вимогам Executive Order 14110 (США) щодо запобігання дискримінації в алгоритмах відбору та вимогам КНР щодо регулювання алгоритмів рекомендацій та розкриття навчальних датасетів.
3. Розробка комплаєнс-пакету для EU AI Act: визначити обов'язкові елементи регуляторного відповідності для High-Risk III (система управління ризиками, якість навчальних даних, технічна документація, реєстрація в базі даних ЄС, забезпечення людського нагляду (human-in-the-loop) та прозорість алгоритмів).
4. Інтеграція з українською Дорожньою картою та Soft Law: проаналізувати Білу книгу та методичні рекомендації Мінцифри України, підготувати рекомендації щодо використання інструментів м'якого права (Soft Law) на перехідному етапі.
5. Проєктування участі в регуляторній пісочниці (Regulatory Sandbox): розробити план-заявку для апробації 'TalentScan AI' в українському регуляторному середовищі з метою правового тестування алгоритмів прозорості, мінімізації предвзятості (bias) та захисту персональних даних.

Критерії оцінювання:

Добре: Студент правильно визначив категорію ризику за EU AI Act та запропонував основні кроки комплаєнсу, детально описав українську Дорожню карту, але допустив незначні неточності у порівняльному аналізі законодавства США чи Китаю або розробці вимог до прозорості алгоритму.

Відмінно: Студент безпомилково кваліфікував категорію ризику за EU AI Act (виявлено елементи High-Risk та розкрито нюанси заборони розпізнавання емоцій), провів глибокий порівняльний аналіз регулювання в США та Китаї, повністю розробив алгоритм дій для участі в регуляторній пісочниці України та правильно застосував інструменти Soft/Hard Law.

Задовільно: Студент загалом орієнтується у нормах EU AI Act та Дорожній карті України, проте припустився помилок у класифікації ризику системи III, поверхово описав поняття регуляторної пісочниці та не навів конкретних механізмів забезпечення прозорості алгоритмів.

Рекомендації для самостійної роботи

Під час опрацювання теми зосередьте увагу на порівняльному аналізі ризик-орієнтованого підходу EU AI Act з децентралізованою моделлю США (EO 14110, стандарти NIST) та державно-центричним контролем Китаю. Детально проаналізуйте Дорожню карту регулювання ШІ в Україні, оцінивши поетапний перехід від інструментів Soft Law до Hard Law, а також юридичний механізм функціонування регуляторних пісочниць (Regulatory Sandboxes) для тестування HR-Tech та інших високоризикових AI-систем.

Питання для самоконтролю:

Які критерії класифікації систем штучного інтелекту за рівнем ризику встановлені Регламентом (ЄС) 2024/1689 (EU AI Act), та які специфічні юридичні зобов'язання (зокрема, щодо людського нагляду та оцінки відповідності) покладаються на розробників систем високого ризику?

У чому полягає принципова відмінність між підходами Soft Law та Hard Law у контексті реалізації Дорожньої карти з регулювання ШІ в Україні, та як це впливає на гармонізацію національного законодавства з *acquis communautaire* ЄС?

Як інститут регуляторних пісочниць (Regulatory Sandboxes) дозволяє збалансувати правові ризики порушення приватності й алгоритмічної упередженості з необхідністю стимулювання інновацій для AI-стартапів?

Завдання для самостійної роботи:

Проведіть комплаєнс-аудит HR-Tech системи автоматизованого рекрутингу та відбору кандидатів відповідно до вимог EU AI Act: визначте категорію ризику системи, сформулюйте перелік необхідної технічної документації та розробіть проект внутрішнього регламенту людського нагляду (human oversight).

Розробіть проект заявки та правову концепцію для участі українського розробника AI-рішення у національній регуляторній пісочниці (Regulatory Sandbox): опишіть потенційні правові ризики технології, запропонуйте заходи з забезпечення прозорості алгоритмів та мінімізації дискримінаційних ризиків.

YouTube, онлайн-курси та корисні ресурси

Офіційний текст EU AI Act (Regulation (EU) 2024/1689) на EUR-Lex - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

Офіційний вебпортал Міністерства цифрової трансформації України - <https://thedigital.gov.ua/>

NIST AI Risk Management Framework - <https://www.nist.gov/itl/ai-risk-management-framework>

Семінар по темі 4(3). Генеративний ШІ та промпт-інжиніринг для юристів. Аналіз документів та даних за допомогою ШІ (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. Аналіз суперечливих показань свідків та умов договору через анти-анкеринг, CoT та Chain-of-Verification

Фабула справи: Юрист представляє інтереси ТОВ «Логістик Груп» у господарському спорі про стягнення збитків за пошкодження товару під час зберігання на складі Орендодавця (ТОВ «Склад Сервіс»). У матеріалах справи є розлого протокольовані показання двох свідків (начальника складу та водія), які містять внутрішні суперечності щодо часу виникнення протікання даху, а також складний 25-сторінковий Договір о відповідальному зберіганні з численними додатковими угодами. Завдання студента: побудувати юридично безпечний процесуальний аналіз матеріалів за допомогою ШІ (ChatGPT / Claude), мінімізуючи ризик галюцинацій та ефект якоріння.

Алгоритм обговорення:

Формулювання власних первинних гіпотез щодо суперечностей у показаннях (техніка анти-анкерингу) ДО введення даних у ШІ та зафіксування їх у робочому щоденнику.

Побудова базованого на структурі «Персона → Контекст → Проблема» промпту із додаванням явних заборон (negative constraints: заборона домислювати факти, яких немає в тексті).

Застосування техніки Prompt Decomposition: окремий аналіз договорів за блоками відповідальності та окремий аналіз показань свідків.

Запуск ланцюжка покрокових міркувань (Chain-of-Thought) для співставлення часових часових ліній (timeline) з двох протоколів показань свідків.

Застосування алгоритму Chain-of-Verification (CoVe): примусове генерування моделлю 3–4 верифікаційних питань до власної відповіді для перевірки фактів перед формулюванням остаточного висновку.

Проведення «тесту на спрощення» для виявлення ефекту планаризації (втрати важливих юридичних нюансів) та фіксація метаданих запиту (інструмент, версія моделі, промпт).

Критерії оцінювання:

Добре: Студент правильно склав структурований промпт та використав техніку CoT, проте пропустив етап анти-анкерингу або неповністю застосував

алгоритм самоперевірки CoVe. Висновки ІІІ оцінено критично, але фіксація параметрів запиту здійснена частково.

Відмінно: Студент демонструє повне розуміння методики: сформував власну гіпотезу до аналізу ІІІ (анти-анкеринг), склав точний промпт за схемою «Персона-Контекст-Проблема» з явними заборонами, успішно застосував декомпозицію, CoT та алгоритм CoVe. Виявлено всі суперечності в показаннях, сформовано критичну оцінку висновків ІІІ із фіксацією параметрів запиту та відновленням втраченого контексту.

Задовільно: Студент використав базовий запит без чіткого розмежування структури (Персона/Контекст/Проблема) та без обмежень на галюцинації. Результат ІІІ прийнято як готовий висновок із мінімальною критичною корекцією, допущено ефект планаризації (втрату нюансів справи).

Кейс 2. Парсинг та автоматизований аналіз масиву судових рішень через Few-Shot Prompting та генерацію Python-коду

Фабула справи: Адвокатському бюро необхідно підготувати узагальнення судової практики з 100+ рішень у справах про перевищення повноважень директором ТОВ при укладенні значних правочинів (ст. 44 ЗУ «Про товариства з обмеженою та додатковою відповідальністю»). Масив рішень експортовано у неупорядкованому виврузі (файли .txt/.csv). Завдання студента: використати генеративний ІІІ як інструмент написання та виконання Python-скрипту для очищення й структурування даних, після чого застосувати Few-Shot Prompting для створення підсумкової класифікаційної таблиці судом застосованих критеріїв добросовісності контрагента.

Алгоритм обговорення:

Сформулювати інструкцію для генеративного ІІІ (наприклад, Advanced Data Analysis / Code Interpreter) щодо створення Python-скрипту для парсингу та очищення тексту судових рішень від формального сміття.

Запустити згенерований код, виконати перевірку та нормалізацію масиву даних (структурування по датах, судах, результату розгляду).

Розробити промпт із використанням техніки Few-Shot Prompting (надати ІІІ 2–3 зразки ідеально розібраних рішень) для стандартизованого витягу юридично значущих фактів з кожного рішення.

Застосувати RAG-підхід (або симуляцію через роботу з контекстним вікном) для категоризації судових рішень за позицією суду щодо «добросовісності третьої особи».

Провести оцінку ризику дескілінгу та епістемічної дистанції: вручну перевірити вибірку з 5% рішень на предмет правильності категоризації моделлю.

Сформувати підсумкову аналітичну записку, трактуючи згенерований результат як робочу чернетку.

Критерії оцінювання:

Добре: Студент успішно згенерував код та застосував Few-Shot Prompting, але допустив незначні помилки у структуризації закритих категорій або виконана вибіркова перевірка результатів була поверхневою.

Відмінно: Студент безпомилково сформулював завдання для генерації Python-скрипту, успішно очистив дані, склав точний Few-Shot промпт із коректними прикладами. Проведено ручний аудиторський контроль (подолання епістемічної дистанції) та сформовано високоякісний аналітичний звіт без викривлення судової практики.

Задовільно: Студент створив функціональний промпт для коду, але не застосував Few-Shot Prompting, через що згенерована таблиця має нестандартний/неупорядкований формат. Критична перевірка результатів генерації та аналіз помилок відсутні.

Рекомендації для самостійної роботи

Під час опрацювання теми рекомендовано послідовно опанувати трикомпонентний фреймворк «Персона → Контекст → Проблема», відпрацювавши прийоми анти-анкерінгу для збереження об'єктивності правової оцінки. Окрему увагу слід приділити практичному застосуванню алгоритмів Chain-of-Thought та Chain-of-Verification при деталізованому аналізі документів, а також критичній оцінці ризиків планаризації й дескілінгу при роботі з RAG-системами та генерацією коду для аналізу даних.

Питання для самоконтролю:

Яким чином методологія анти-анкерінгу та формулювання явних заборон у юридичному промпті запобігають когнітивним викривленням правника та підтверджувальному упередженню ШІ під час розбору доказів і показань свідків?

У чому полягає відмінність між інженерними техніками Few-Shot Prompting, Chain-of-Thought (CoT) та Chain-of-Verification (CoVe), і як їх комбінація дозволяє мінімізувати галюцинації алгоритмів при складанні процесуальних документів?

Як використання RAG-архітектури та генерації коду (Python/SQL) впливає на епістемічну дистанцію юриста з правовими джерелами, і за допомогою яких інструментів (зокрема «тесту на спрощення») долається ефект планаризації юридичних нюансів?

Завдання для самостійної роботи:

Складіть комплексний юридичний промпт за схемою «Персона → Контекст → Проблема» з імплементацією правил анти-анкерінгу та алгоритму Chain-of-Thought (CoT) для первинного розбору суперечливих показань свідків у цивільній справі, передбачивши етап самоперевірки за принципом Chain-of-Verification (CoVe).

Розробіть Few-Shot промпт для витягування та уніфікації істотних умов із масиву договорів поставки, після чого сформулюйте запит до ШІ на генерацію Python-скрипту для структурування цих даних у JSON-формат із суворим контролем недопущення домислювання фактів.

YouTube, онлайн-курси та корисні ресурси

Посібник з промпт-інжинірингу OpenAI (Prompt Engineering Guide) - <https://platform.openai.com/docs/guides/prompt-engineering>

Інтерактивна документація Anthropic з побудови промптів для складного аналізу - <https://docs.anthropic.com/en/docs/build-with-claude/prompt-engineering/overview>

Єдиний державний реєстр судових рішень України - <https://reyestr.court.gov.ua/>

Семінар по темі 5(4). Штучний інтелект у державному управлінні та електронному урядуванні (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. «SmartAssist-Social»: межі людського нагляду (Human-in-the-Loop) та автоматизоване призупинення соціальних виплат

Центральний орган виконавчої влади запровадив алгоритмічну систему «SmartAssist-Social» для виявлення шахрайства при призначенні соціальних допомог. Система аналізує реєстри та привласнює кожному одержувачу балу «ризикую зловживань». У разі досягнення показника 85/100 система генерує проект рішення про призупинення виплат. Соціальний інспектор витрачає в середньому 25 секунд на перегляд справи і натискає кнопку «Затвердити», після чого громадянин N (особа з інвалідністю) отримує автоматичне сповіщення про призупинення допомоги без пояснення конкретних причин, окрім посилання на «високий коефіцієнт алгоритмічного ризику». Громадянин

Н оскаржує рішення, стверджуючи про порушення ст. 22 GDPR, відсутність належної правової процедури (Due Process) та відсутність змістовного людського втручання. Орган влади заявляє, що рішення прийнято інспектором, а отже, ст. 22 GDPR не застосовується.

Алгоритм обговорення:

Здійснити правову кваліфікацію рішення органу влади через призму прецедентної практики Суду ЄС у справі Schufa (C-634/21), встановивши, чи є залучення інспектора на 25 секунд «змістовним людським наглядом» чи формальним затвердженням.

Проаналізувати дотримання вимог статті 22 GDPR та презумпції незаконності повної автоматизації в публічному секторі, оцінивши наявність/відсутність законних виключень.

Оцінити правомірність дій органу влади крізь призму принципу належної правової процедури (Due Process) та правових висновків справи MiDAS (Bauserman v. Michigan UIA).

Сформулювати вимоги щодо забезпечення «права на пояснення» (проста форма, відносна вага факторів) та захисту вразливих груп відповідно до концепції когнітивного суверенітету Л. Байгрейва.

Розробити пропозиції щодо переформатування системи за критеріями EU AI Act (високий ризик) та запровадження реальної концепції «Human-in-the-Loop».

Критерії оцінювання:

Добре: Студент правильно кваліфікував порушення ст. 22 GDPR та принципів Human-in-the-Loop, згадав релевантну судову практику, проте припустився незначних неточностей у розмежуванні формального та змістовного нагляду або не повністю розкрив критерії «права на пояснення».

Відмінно: Студент детально проаналізував кейс з використанням практики Schufa (C-634/21) та MiDAS, аргументовано довів формальний характер втручання інспектора (гуманоїдний штамп), правильно застосував ст. 22 GDPR, обґрунтував порушення права на пояснення та когнітивного суверенітету, висунув точні методичні пропозиції щодо гармонізації з EU AI Act.

Задовільно: Студент дав загальний аналіз ситуації, встановив наявність порушення прав громадянина, але проігнорував правові позиції Суду ЄС (справа Schufa) або не зміг аргументувати юридичний зв'язок між рішенням алгоритму та посадової особи.

Кейс 2. «ReguAI-Draft»: алгоритмічний аналіз громадських консультацій та проблема алгократії в нормотворчості

Міністерство розвитку громад застосувало спеціалізовану генеративну модель ШІ «ReguAI-Draft» для опрацювання 15 000 пропозицій громадян, поданих під час онлайн-консультацій щодо нового зонінгу територій. Система узагальнила звернення, згрупувала їх за категоріями та автоматично згенерувала підсумковий аналітичний звіт і проект нормативно-правового акта. Згодом з'ясувалося, що через ефект «галюцинацій» та викривлення алгоритмом вагових коефіцієнтів, критичні зауваження вразливих груп (осіб з інвалідністю та представників місцевих корінних спільнот) були систематично відфільтровані як «статистичний шум». Депутати міської ради затвердили проект акта без істотних змін, покладаючись на «об'єктивність аналізу ШІ». Громадські організації заявили про кризу демократичної легітимності рішення, загрозу алгократії та дескілінг посадовців.

Алгоритм обговорення:

Дослідити проблему використання ШІ в нормотворчості через призму концепцій алгократії (А. Фердман) та епістемічної дистанції між громадянами та суб'єктом владних повноважень.

Проаналізувати ризики алгоритмічної дискримінації вразливих груп та оцінити дотримання принципу алгоритмічної підзвітності за матеріалами звіту OECD «Governing with Artificial Intelligence».

Здійснити порівняльний аналіз профілю ризику використання ШІ в нормотворчості порівняно з прийняттям індивідуальних адміністративних актів.

Використовуючи досвід кейсу Amsterdam Smart Check, оцінити функціональні збої алгоритму та запропонувати механізми аудиту входження даних і процедури людської перевірки (Human Oversight).

Сформулювати юридично обґрунтований алгоритм забезпечення авторства норми та збереження когнітивного суверенітету суб'єктів нормотворчості.

Критерії оцінювання:

Добре: Студент правильно визначив юридичні та етичні проблеми застосування ШІ в нормотворчості, проаналізував ризики дискримінації вразливих груп, але поверхово розкрив теоретичні засади алгократії або надав узагальнені рекомендації щодо аудиту ШІ.

Відмінно: Студент продемонстрував глибоке розуміння теоретичних викликів алгоритмічного урядування (алгократія, епістемічна дистанція, дескілінг),

фахово проаналізував кейс через звіт OECD та концепцію когнітивного суверенітету, розробив детальний механізм алгоритмічної підзвітності в нормотворчому процесі.

Задовільно: Студент виявив розуміння наявності помилок у роботі ШІ, проте аналіз обмежився загальними фразами про недосконалість технологій без застосування спеціального понятійного апарату (алгократія, підзвітність, оцінка ризиків EU AI Act).

Кейс 3. «Amsterdam Smart Check»: аналіз причин згорання проєкту та розробка концепції алгоритмічного ризик-менеджменту в Україні

Муніципалітет Амстердама розробив та тестував алгоритмічну систему «Smart Check» для автоматизованого виявлення зловживань і шахрайства при отриманні соціальних виплат та муніципального житла. Система опрацьовувала декілька категорій персональних даних та будувала профілі ризику громадян. Однак через хвилю правозахисної критики, ризики дискримінації та профілювання за непрозорими критеріями, відсутність належної правової основи й загрозу втрати довіри до влади муніципалітет ухвалює рішення про повне припинення проєкту та перехід до моделі публічного Реєстру алгоритмів (Algorithm Register). Вивчаючи європейський досвід, робоча група Міністерства цифрової трансформації України розглядає можливість впровадження аналогічної системи ризик-орієнтованого моніторингу соціальних виплат. Студентам пропонується виступити в ролі юридичних експертів для аналізу амстердамського досвіду та підготовки нормативних пропозицій.

Алгоритм обговорення:

Проаналізувати передумови створення, правові підстави та ключові причини закриття проєкту «Amsterdam Smart Check» (алгоритмічне профілювання, непрозорість критеріїв, ризики алгоритмічного упередження та дискримінації).

Оцінити правомірність використання подібних систем крізь призму вимог EU AI Act (високий ризик систем у сфері доступності соціальних послуг) та статей 5, 6, 22 GDPR.

Дослідити інституційну трансформацію Амстердама від закритих моделей до відкритості через Публічний реєстр алгоритмів (Algorithm Register) та концепцію Algorithmic Transparency.

Розробити пропозиції та правові запобіжники щодо можливої реалізації аналогічної системи ризик-орієнтованого моніторингу в Україні, враховуючи

вимоги Закону України «Про захист персональних даних», принципи належного врядування та права на оскарження.

Сформулювати проєкт вимог до людського нагляду (Human Oversight), регулярного алгоритмічного аудиту та забезпечення права громадян на інформацію про алгоритми в публічному секторі.

Критерії оцінювання:

Добре: Студент правильно визначив причини згорання проєкту в Амстердамі, проаналізував ризики дискримінації та порушення GDPR, надав загалом якісні рекомендації щодо реалізації подібних рішень в Україні, але припустився незначних прогалин у нормативній деталізації процедур алгоритмічного аудиту чи human-in-the-loop.

Відмінно: Студент детально проаналізував причини закриття проєкту «Amsterdam Smart Check», виявив систематичні юридичні й етичні вади алгоритмічного профілювання, фахово порівняв модель закритих систем із концепцією Algorithm Register та запропонував якісний, обґрунтований нормативно-правовий алгоритм впровадження подібних інструментів в Україні з повним дотриманням принципів EU AI Act і захисту прав людини.

Задовільно: Студент стисло виклав причини зупинки проєкту Amsterdam Smart Check та надав базові пропозиції для України, проте аналіз має переважно описовий характер без належного застосування юридичних норм (EU AI Act, GDPR, українське законодавство) та без системного урахування правових запобіжників.

Рекомендації для самостійної роботи

При опрацюванні теми зосередьтеся на системному аналізі ст. 22 GDPR та положень EU AI Act щодо класифікації систем публічного управління як систем високого ризику. Окрему увагу приділіть розмежуванню формального затвердження рішення алгоритмом та змістовного людського нагляду (Human-in-the-Loop) на прикладі судової практики (справи Schufa C-634/21 та Bauserman v. Michigan UIA). Дослідіть юридичні гарантії дотримання принципу належної правової процедури (Due Process) та запобігання ризикам алгократії при використанні ІІІ у нормотворчості й наданні публічних послуг.

Питання для самоконтролю:

Як правова позиція Суду ЄС у справі Schufa (C-634/21) трансформувала розуміння поняття «рішення» у ст. 22(1) GDPR та чому вона унеможливило формальне залучення людини («гумова печатка») для обходу заборони автоматизованого управління?

У чому полягає конфлікт між концепцією когнітивного суверенітету Л. Байгрейва та епістемічною дистанцією у разі застосування алгоритмічних систем у нормотворчому процесі та формуванні публічної політики?

За якими критеріями у контексті EU AI Act та звіту OECD «Governing with AI» здійснюється класифікація систем ШІ в публічному секторі як систем високого ризику, та які обов'язкові механізми оцінки ризиків дискримінації вразливих груп мають бути запроваджені?

Завдання для самостійної роботи:

Проведіть правовий аудит кейсу «SmartAssist-Social» (або MiDAS): сформулюйте юридичний висновок (legal opinion) щодо відповідності автоматизованого призупинення соціальних виплат вимогам принципу належної правової процедури (Due Process), ст. 22 GDPR та концепції змістовного людського нагляду (Human-in-the-Loop).

Розробіть проект Концепції алгоритмічного ризик-менеджменту та підзвітності для органів місцевого самоврядування України, адаптувавши досвід та причини згорання проєкту «Amsterdam Smart Check», із визначенням критеріїв прозорості, права на пояснення та запобігання алгократії.

YouTube, онлайн-курси та корисні ресурси

Офіційний текст Загального регламенту про захист даних (GDPR) на порталі EUR-Lex - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Офіційний текст Акта ЄС про штучний інтелект (EU AI Act) на порталі EUR-Lex - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Аналітична платформа ОЕСР з питань політики у сфері штучного інтелекту (OECD.AI) - <https://oecd.ai/>

Семінар по темі 6(5). Приватно-правовий контекст ШІ. Право не бути суб'єктом автоматизованих рішень. Автоматизація договірної роботи. Авторське право та ШІ (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. «Оскарження автоматизованого скорингу та відмови у наданні кредиту (Застосування ст. 22 GDPR)»

Громадянин Олексій звернувся до приватного банку «FinTech Bank» через мобільний застосунок із заявою про надання іпотечного кредиту на суму 2 000 000 грн. За декілька секунд після відправки анкети застосунок видав

автоматичну відмову. Як з'ясувалося згодом, банк використовує алгоритм глибокого навчання (Machine Learning) для оцінки кредитоспроможності, який здійснює профайлінг заявників на основі аналізу їхньої історії покупок, активності в соціальних мережах, геолокаційних даних та поштового індексу місця проживання. Олексій звернувся до банку з вимогою надати пояснення логіки прийнятого рішення, провести повторний розгляд заяви людиною та виплатити компенсацію за незаконний профайлінг. Банк відмовив, заявивши, що алгоритм є комерційною таємницею, а використання ШІ передбачене Публічною офертою (Угодою користувача), яку Олексій акцептував під час реєстрації в застосунку.

Алгоритм обговорення:

Проаналізувати нормативно-правове підґрунтя застосування ст. 22 GDPR (або відповідного національного законодавства) до відносин між клієнтом та приватним банком.

Визначити, чи підпадає оцінка кредитоспроможності ШІ під критерії «рішення, яке базується виключно на автоматизованій обробці, включаючи профайлінг» та має «юридичні наслідки або істотно впливає на особу».

Оцінити законність покликання банку на Публічну оферту як на виняток щодо згоди суб'єкта даних або необхідності укладення договору (ст. 22(2) GDPR).

Перевірити дотримання банком прав суб'єкта даних: права на отримання людського втручання (human intervention), права висловити власну точку зору та оскаржити рішення (ст. 22(3) GDPR).

Проаналізувати баланс між захистом прав персональних даних / прозорістю алгоритму (Explainable AI) та збереженням комерційної таємниці / інтелектуальної власності банку на ШІ-модель.

Сформулювати підсумковий юридичний висновок та алгоритм захисту прав клієнта або правовий висновок для банку щодо мінімізації регуляторних ризиків.

Критерії оцінювання:

Добре: Студент правильно визначив суть проблеми автоматизованого рішення та профайлінгу; зробив посилання на нормативні акти, проте припустився незначних похибок у розмежуванні винятків ст. 22(2) GDPR або в обґрунтуванні балансу між прозорістю алгоритму та комерційною таємницею.

Відмінно: Студент надав вичерпну та юридично обґрунтовану кваліфікацію дій банку; вірно застосував ст. 22 GDPR та концепцію 'human-in-the-loop';

детально розмежував поняття комерційної таємниці та права на пояснення (right to explanation); запропонував чіткий алгоритм дій для обох сторін.

Задовільно: Студент поверхово описав ситуацію, визначив лише базові права клієнта без належного правового аналізу GDPR, припустився помилок у кваліфікації угоди користувача як підстави для автоматизованої обробки даних.

Кейс 2. «Алгоритмічний збій автономного ШІ-агента у смарт-контракті та розподіл цивільно-правової відповідальності»

Компанія «Logistics Hub» (Покупець) уклала договір на постачання пального з ТОВ «Fuel Trade» (Продавець). Для автоматизації закупівель Покупець інтегрував автономного ШІ-агента у децентралізований смарт-контракт на базі блокчейн. ШІ-агент мав моніторити біржові ціни на пальне та самостійно підписувати електронні замовлення при зниженні ціни нижче заданого порогу. Внаслідок аномального некоректного оновлення зовнішнього джерела даних (оракула) та внутрішньої помилки алгоритму адаптивного навчання, ШІ-агент сформував замовлення на закупівлю обсягу пального, який у 50 разів перевищує складські потужності Покупця, за ціною, що втричі перевищувала ринкову. Смарт-контракт автоматично списав з криптовалютного рахунку Покупця 1,5 млн USDT на користь Продавця. Покупець звернувся до суду з позовом про визнання правочину недійсним через відсутність реального волевиявлення та стягнення збитків. У відповідь розробник ШІ-програми заявив, що ШІ діяв автономно як «квазі-суб'єкт», а Продавець стверджує, що виконував детермінований смарт-контракт за принципом «код є закон» (code is law).

Алгоритм обговорення:

Здійснити правову кваліфікацію статусу автономного ШІ-агента у договірному праві (інструмент/засіб укладення договору, агентська модель чи джерело підвищеної небезпеки).

Проаналізувати питання наявності та належності волевиявлення сторін при укладенні правочинів через автономні алгоритми.

Оцінити можливість застосування норм цивільного законодавства про помилку під час укладення правочину (помилка в розрахунках, технічний збій коду).

Визначити правову природу принципів функціонування смарт-контрактів та їх співвідношення із класичними інститутами договірного права.

Здійснити розподіл цивільно-правової відповідальності за завдані збитки між Покупцем (користувачем ШІ), Продавцем та розробником ШІ-агента (виробничий дефект/недбалість).

Скласти проект резолютивної частини судового рішення за позовом Компанії «Logistics Hub».

Критерії оцінювання:

Добре: Студент вірно кваліфікував ШІ-агента як інструмент волевиявлення та вказав на наявність помилки правочину, проте неповністю аргументував відповідальність розробника програмного забезпечення або оракула.

Відмінно: Студент продемонстрував глибоке розуміння концепцій квазі-правосуб'єктності, теорії волевиявлення та специфіки смарт-контрактів; проаналізував моделі розподілу відповідальності (продуктова відповідальність, джерело підвищеної небезпеки, делікт) та надав коректний розв'язок спору.

Задовільно: Студент дав поверхневу оцінку ситуації, визнав ШІ повноцінним суб'єктом права без належного юридичного обґрунтування або обмежився формальним посиланням на принцип «код є закон».

Кейс 3. «Спор про авторські права на AI-generated content та законність Text and Data Mining (TDM)»

Спілка художників «Digital Art Guild» подала колективний позов проти технологічної компанії «Neural Gen», розробника нейромережі для генерації зображень «ArtVision». Позивачі стверджують, що відповідач без їхньої дозволу та без виплати винагороди використовував мільйони їхніх авторських картин для навчання моделі (Text and Data Mining), чим порушив їхні виключні майнові права. Крім того, користувачі «ArtVision», вказуючи промпт «картина у стилі [Ім'я Відомого Художника]», отримують згенеровані арт-об'єкти, які продаються на NFT-маркетплейсах. «Neural Gen» у захисті покликається на концепцію добросовісного використання (Fair Use / TDM exception) для навчання ШІ, а також стверджує, що згенеровані зображення є повністю новими об'єктами, авторські права на які належать користувачам, які сформували промпт.

Алгоритм обговорення:

Проаналізувати правовий режим використання об'єктів авторського права для навчання мовних та генеративних моделей (Text and Data Mining) згідно із законодавством ЄС (CDSM Directive) та/або США (Fair Use doctrine).

Дослідити наявність чи відсутність прямого порушення авторських прав при копіюванні творів у пам'ять ШІ під час його тренування.

Проаналізувати правовий статус згенерованого контенту (AI-generated content): вимогу людського авторства (human authorship requirement) та рівень творчого внеску через промпт-інжиніринг.

Оцінити наявність істотної подібності (substantial similarity) між оригінальними творами художників та згенерованим результатом.

Визначити, чи виникають авторські права на твори, створені за допомогою ШІ, та кому вони належать (розробнику, користувачу чи переходять у суспільне надбання).

Сформулювати правову позицію для судового захисту кожної зі сторін спору.

Критерії оцінювання:

Добре: Студент вірно розкрив поняття навчання ШІ та проблеми авторського права на AI-контент, правильно визначив відсутність авторства у самого ШІ, але припустився окремих неточностей при аналізі доктрини Fair Use або TDM-директиви ЄС.

Відмінно: Студент надав критичний аналіз концепцій TDM-винятків, доктрини Fair Use та критерію людського авторства; навів релевантну міжнародну судову практику (наприклад, справи *Andersen v. Stability AI*, *Thaler v. Perlmutter*); зробив чіткі обґрунтовані висновки щодо долі авторських прав на промпти та результати генерації.

Задовільно: Студент описово виклав позиції сторін, визнав авторські права за штучним інтелектом або користувачем лише на підставі написання промпту без глибокого правового аналізу критерію творчого внеску.

Рекомендації для самостійної роботи

Під час опрацювання теми зосередьте увагу на межах застосування ст. 22 GDPR у відносинах між приватними суб'єктами та механізмах забезпечення гарантії «human-in-the-loop» при залученні скорингових чи HR-алгоритмів. Порівняйте доктринальні концепції «електронної особи» (electronic person) та джерела підвищеної небезпеки для розподілу цивільно-правової відповідальності за збої автономних ШІ-агентів. Дослідіть правовий режим AI-generated content та винятки Text and Data Mining (TDM) через призму балансу інтересів правовласників і розробників великих мовних моделей.

Питання для самоконтролю:

Які юридичні критерії розмежовують виключно автоматизоване прийняття рішень (ст. 22 GDPR) від рішень за участю людини (human-in-the-loop), та як це застосовується у банківському скорингу й алгоритмічному наймі?

У чому полягає юридична специфіка волевиявлення та розподілу ризиків при укладенні договорів автономними ШІ-агентами через смарт-контракти у разі алгоритмічного збою чи помилки в коді?

Які підходи застосовуються у міжнародному та європейському праві щодо надання авторсько-правової охорони об'єктам, згенерованим ШІ (AIGC), та в чому полягає суть правового режиму Text and Data Mining (TDM) при навчанні нейромереж?

Завдання для самостійної роботи:

Складіть проєкт звернення (скарги) від імені клієнта до банківської установи на підставі ст. 22 GDPR з вимогою перегляду рішення про відмову у наданні кредиту, прийнятого виключно автоматизованою системою скорингу, сформулювавши аргументацію щодо обов'язкового залучення людини (human-in-the-loop).

Проведіть юридичний аналіз (правовий аудит) проєкту договору про розробку та впровадження автономного ШІ-агента для автоматизації закупівель: розробіть застереження про розподіл цивільно-правової відповідальності та ризиків між розробником, замовником і користувачем на випадок збою або помилки алгоритму.

YouTube, онлайн-курси та корисні ресурси

Офіційний текст GDPR на порталі EUR-Lex - <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Розділ Всесвітньої організації інтелектуальної власності (WIPO) про ШІ та інтелектуальну власність - https://www.wipo.int/about-ip/en/artificial_intelligence/

Офіційний сайт Європейської ради з захисту даних (EDPB) - <https://edpb.europa.eu/>

Семінар по темі 7(6). ШІ та кримінально-правове регулювання. Використання ШІ для вчинення злочинів. ШІ в діяльності правоохоронних органів та судів (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. Процесуальна допустимість доказів, отриманих за допомогою мультимодальної ІІІ-платформи 'Longeye' (Проблема «чорної скриньки» та стандарти справедливого суду)

Під час розслідування серії квартирних крадіжок орган досудового розслідування застосував аналітичну платформу ІІІ «Longeye» для опрацювання понад 500 годин відеозаписів із приватних та муніципальних камер спостереження, а також боді-камер поліцейських. Система встановила цифровий збіг ходака (gait analysis) та силуету підозрюваного Г. із фігурантом трьох епізодів, а також згенерувала транскрипт аудіозапису виклику на лінію 102 із висновком про 94% ймовірність належності голосу підозрюваному. Слідчий залучив підсумковий звіт ІІІ-платформи до матеріалів кримінального провадження як безпосередній електронний доказ. Захист заявив клопотання про визнання цього звіту недопустимим доказом, оскільки: 1) розробник платформи відмовився розкрити вихідний код алгоритму, посилаючись на комерційну таємницю (проблема «чорної скриньки» / black box); 2) слідчий повністю поклався на автоматизований висновок без проведення відповідної судової фототехнічної чи фоноскопичної експертизи; 3) це порушує право на захист та принцип рівності сторін, оскільки сторона захисту позбавлена можливості піддати перехресному допиту або критичному аналізу алгоритм ІІІ (аналогія зі справою Loomis). Оцініть процесуальний статус звіту ІІІ та правомірність клопотання захисту з урахуванням EU AI Act та ст. 22 GDPR.

Алгоритм обговорення:

Здійснити юридичну кваліфікацію статусу ІІІ-платформи: розмежувати ІІІ як ординарний 'інструмент пошуку/орієнтуючу інформацію' та ІІІ як джерело самостійного процесуального доказу.

Проаналізувати висновок ІІІ на відповідність вимозі 'змістовного людського контролю' (Meaningful Human Control): оцінити, чи виступав слідчий суб'єктом прийняття рішення, чи відбулося сліпе перенесення алгоритмічного висновку в процесуальний документ.

Оцінити проблему 'чорної скриньки' (Black Box) крізь призму прецедентної практики (зокрема справи State v. Loomis) та ст. 6 Конвенції про захист прав людини і основоположних свобод (право на справедливий суд та доступ до матеріалів).

Перевірити дотримання вимог EU AI Act щодо систем ІІІ високого ризику (High-Risk AI Systems) в сфері правоохоронної діяльності (вимоги щодо прозорості, реєстрації дій, простежуваності та пояснюваності).

Сформулювати підсумкове процесуальне рішення (ухвалу слідчого судді/суду) щодо задоволення або відмови в задоволенні клопотання про визнання доказу недопустимим із чітким алгоритмом усунення процесуальних недоліків (призначення судової експертизи).

Критерії оцінювання:

Добре: Студент вірно визначив відсутність у звіту ІІІ автоматичного статусу доказу, вказав на необхідність судово-експертного підтвердження та людського контролю, згадав про прозорість алгоритмів, але припустився незначних точечних прогалин у юридичній аргументації щодо міжнародних стандартів чи прецедентної практики.

Відмінно: Студент детально та аргументовано розмежував процесуальний статус ІІІ як пошукового інструменту та джерела доказів; глибоко проаналізував проблему 'чорної скриньки' зі посиланням на справу Loomis та стандарти ст. 6 ЄКПЛ; застосував положення EU AI Act та ст. 22 GDPR щодо змістовного людського контролю; сформулювати бездоганне процесуальне рішення.

Задовільно: Студент поверхнево оцінив висновок ІІІ, вказав лише на загальні проблеми недопустимості доказів або копіювання текстів нормативних актів без глибокого правового аналізу проблеми 'чорної скриньки' та відсутності людського контролю.

Кейс 2. Дискримінаційні ризики предиктивного патрулювання та біометричної ідентифікації (Уроки систем HART, PredPol та справи Роберта Вільямса)

У місті М. поліцейський департамент впровадив систему предиктивної поліцейської діяльності 'Predict-Crime', яка аналізує історичні дані про правопорушення для визначення 'гарячих точок' (hotspots), та алгоритм розпізнавання облич для патрульних дронів. Через 6 місяців аналіз показав, що 80% затримань у 'гарячих точках' припадає на національні меншини, які мешкають у бідних районах, хоча загальна статистика латентної злочинності за самозвітами громадян є рівномірною по всьому місту. На основі спрацювання розпізнавання облич з деталізацією лише 62% (через низьку якість камери дрона) патрульні затримали громадянина К., застосували до нього запобіжний захід та утримували в підрозділі 30 годин, після чого з'ясувалося, що це помилка ідентифікації (подібно до справи Роберта Вільямса, Детройт, 2020/2024). Громадянин К. подав позов про компенсацію шкоди та заборону використання системи, заявляючи про дискримінацію, порушення презумпції невинуватості та застосування 'алгоритмічного усереднення'. Проаналізуйте правові наслідки ефекту 'зворотної петлі'

(feedback loop) та висуніть вимоги до розробки мирової угоди за аналогією з детройтським прецедентом 2024 року.

Алгоритм обговорення:

Розкрити феномен 'алгоритмічного усереднення' та ефекту 'зворотної петлі' (feedback loop): пояснити, як історично упереджені дані поліцейської статистики про повторні арешти створюють самопідтверджувальні хибні прогнози в предиктивних системах (на прикладі досліджень HRDAG щодо PredPol та системи HART).

Проаналізувати відповідність застосування розпізнавання облич в реальному часі вимогам EU AI Act (категорична заборона або виняткові підстави для біометричної ідентифікації у публічному просторі).

Оцінити порушення фундаментальних прав громадянина К. (презумпція невинуватості, свобода від дискримінації, право на свободу та особисту недоторканність).

Розробити юридичні умови Мирової угоди (за зразком урегулювання справи Роберта Вільямса 2024 року): визначити мінімальний поріг якості фото/відео, заборону використання алгоритму як єдиної підстави для арешту, обов'язкову незалежну оцінку біометричних систем та правила аудиту даних.

Критерії оцінювання:

Добре: Студент правильно ідентифікував проблему алгоритмічної дискримінації та помилкової ідентифікації, вказав на недопустимість арешту виключно за підсумком роботи ШІ, однак деталізація рішень або розуміння механізму 'зворотної петлі' розкриті не повною мірою.

Відмінно: Студент продемонстрував виняткове розуміння концепцій 'зворотно-петльового ефекту', 'алгоритмічного усереднення' та систем HART/PredPol; надав чіткий юридичний аналіз порушень прав людини; розробив високопрофесійний проєкт умов мирової угоди на основі Детройтського прецеденту 2024 року та норм EU AI Act.

Задовільно: Студент надав загальний описовий висновок про те, що 'поліція вчинила незаконно', не розкривши специфічні кримінально-процесуальні та технологічні поняття (предиктивна поліція, feedback loop, стандарти біометрії).

Кейс 3. Використання системи COMPAS у судах США: оцінка ризиків рецидивізму, судові прецеденти та етичні виклики алгоритмічного правосуддя

При призначенні покарання та вирішенні питання про дострокове звільнення суди низки штатів США (зокрема Вісконсін) застосовують інструмент COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) для оцінки ризику повторного вчинення злочину. У справі *State v. Loomis* (2016) обвинувачений Ерік Луміс оскаржив вирок, зазначаючи, що використання COMPAS порушує його право на належну правову процедуру (Due Process Clause), оскільки: 1) розробник (Northpointe / Equivant) відмовляється розкрити алгоритм через proprietary-статус (комерційна таємниця); 2) дослідження журналу ProPublica виявило расову упередженість системи (вищий ризик хибнопозитивних результатів для темношкірих обвинувачених). Проведіть комплексне дослідження системи COMPAS, проаналізуйте позитивні та негативні відгуки експертів і практиків, ключовий судовий прецедент *State v. Loomis* та підготуйте аналітичну доповідь про межі допустимості подібних інструментів оцінки ризиків у судочинстві.

Алгоритм обговорення:

Дослідити архітектуру та призначення системи COMPAS: визначити, які дані аналізує алгоритм (психосоціальні анкетні дані, кримінальна історія) та як формується підсумковий бал ризику (risk score).

Систематизувати позитивні відгуки та аргументи на користь COMPAS (зменшення суб'єктивізму судді, стандартизація критеріїв оцінки, індивідуалізація альтернативних запобіжних заходів чи покарань).

Систематизувати критику та негативні відгуки: дослідження ProPublica (2016) щодо racial bias, проблему прозорості (Black Box), ризик перенесення системної дискримінації з минулих даних на майбутнє оцінювання.

Проаналізувати рішення Верховного суду штату Вісконсін у справі *State v. Loomis* (2016): встановити сформульовані судом застереження (cautions/limitations) щодо використання результатів COMPAS (заборона використовувати score як єдину або вирішальну підставу для позбавлення волі).

Підготувати аналітичну доповідь/виступ із рекомендаціями щодо можливості впровадження подібних алгоритмічних оцінок ризиків у національну судову систему із врахуванням гарантій права на справедливий суд.

Критерії оцінювання:

Добре: Студент правильно описав функціонування COMPAS, навів основні позитивні й негативні відгуки, проаналізував прецедент *Loomis* та підготував доповідь, проте припустився незначних прогалин у юридичній аргументації щодо процесуальних гарантій.

Відмінно: Студент надав глибинний аналіз системи COMPAS, фахово систематизував позитивні аргументи та критику (зокрема розслідування ProPublica), детально розкрив правову позицію у справі State v. Loomis із урахуванням гарантій Due Process та підготував високоякісну доповідь із власною виваженою юридичною позицією.

Задовільно: Студент поверхнево висвітлив мету використання COMPAS та рішення у справі Loomis, дав загальний перелік плюсів і мінусів системи без глибокої аналітики та підготував тезисну доповідь без чітких висновків.

Рекомендації для самостійної роботи

Під час самостійного вивчення теми зосередьте увагу на співвідношенні принципу індивідуалізації кримінальної відповідальності та презумпції невинуватості з феноменом «алгоритмічного усереднення» у предиктивній поліцейській діяльності (системи PredPol, HART). Проаналізуйте стандарти допустимості цифрових доказів, отриманих за допомогою мультимодальних ШІ-платформ (зокрема Longeye), крізь призму проблеми «чорної скриньки» (black box problem) та вимог змістовного людського контролю (meaningful human control), визначених у ст. 22 GDPR та EU AI Act. Детально дослідіть судові прецеденти, зокрема справу State v. Loomis та мирову угоду у справі Роберта Вільямса (Детройт, 2024), для розуміння кримінально-процесуальних ризиків використання біометричної ідентифікації.

Питання для самоконтролю:

У чому полягає сутність конфлікту між концепцією «алгоритмічного усереднення» в предиктивному патрулюванні (на прикладі систем PredPol та HART) та фундаментальними принципами презумпції невинуватості й індивідуалізації юридичної відповідальності?

Як ефект «зворотної петлі» (feedback loop) та системне викривлення у вихідних даних (data bias) впливають на виникнення дискримінаційних ризиків при застосуванні технологій розпізнавання облич (FRT) у діяльності правоохоронних органів?

Яким чином проблематика «чорної скриньки» (black box problem) у ШІ-системах оцінки ризиків рецидивізму (на кшталт COMPAS) обмежує право підсудного на справедливий суд та процесуальну рівність сторін відповідно до прецедентної практики (зокрема рішення у справі State v. Loomis)?

Завдання для самостійної роботи:

Складіть юридичний висновок (legal opinion) щодо процесуальної допустимості матеріалів, отриманих за допомогою мультимодальної ШІ-платформи «Longeye» під час розслідування злочину, з урахуванням

розмежування ШІ як «інструменту пошуку» та «джерела доказу», а також вимог гарантій ст. 22 GDPR та EU AI Act.

Здійснить порівняльно-правовий аналіз мирової угоди у справі Роберта Вільямса (Детройт, 2024) та правових обмежень EU AI Act щодо використання систем біометричної ідентифікації в режимі реального часу, сформулювавши пропозиції щодо імплементації цих стандартів у Кримінальний процесуальний кодекс України.

YouTube, онлайн-курси та корисні ресурси

Текст Регламенту ЄС про штучний інтелект (EU AI Act) на порталі EUR-Lex - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Генеральний регламент про захист даних (GDPR, Стаття 22) на порталі EUR-Lex - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Аналітичні дослідження Human Rights Data Analysis Group (HRDAG) щодо предиктивної поліцейської діяльності - <https://hrdag.org/>

Семінар по темі 8 (7). Професійна юридична діяльність та розвиток технологій. LegalTech проєкти на основі ШІ. Правове регулювання квантових обчислень та технологій трансгуманізму (2 год)

Обговорення кейсів у форматі дискусії з попереднім призначенням з числа студентів основного доповідача та рецензентів.

Кейс 1. Професійна етика адвоката, галюцинації ШІ та витік конфіденційних даних через LegalTech-платформу

Адвокатське об'єднання «Право та Інновації» використало корпоративний підписочний LegalTech-сервіс на основі генеративного ШІ (аналог Harvey/CoCounsel) для підготовки складного правового висновку щодо злиття компаній та складання позовної заяви. Прагнучи прискорити роботу, молодий адвокат завантажив у відкриту хмарну модель ШІ первинні документи клієнта, що містили комерційну таємницю та персональні дані керівництва. Крім того, ШІ згенерував кілька правових позицій із посиланням на неіснуючі рішення суду («галюцинації» ШІ). Адвокат не перевіряв згенеровані джерела та подав процесуальні документи до суду. Опонент у судовому засіданні виявив фейкові прецеденти, а за кілька тижнів комерційна таємниця клієнта потрапила у відкритий доступ через витік даних із сервера розробника ШІ. Клієнт ініціював дисциплінарне провадження проти адвоката та позов про відшкодування збитків.

Алгоритм обговорення:

Здійснити юридичний аналіз дій адвоката на предмет дотримання Правил адвокатської етики (зокрема щодо обов'язку компетентності, добросовісності та збереження адвокатської таємниці).

Оцінити процесуальні наслідки надання суду фальсифікованих правових джерел («галюцинацій» ШІ) та ризики притягнення адвоката до відповідальності за неухважність до суду.

Проаналізувати межі відповідальності LegalTech-провайдера та адвокатського об'єднання за порушення режиму захисту комерційної таємниці та персональних даних при використанні хмарних моделей ШІ.

Розробити корпоративний регламент (AI Use Policy) для адвокатського об'єднання щодо допустимих меж та умов використання інструментів ШІ у професійній діяльності.

Критерії оцінювання:

Добре: Студент вірно визначив основні юридичні проблеми (порушення таємниці, процесуальні ризики), але припустився незначних неточностей у розмежуванні відповідальності суб'єктів або запропонував загальний, невизначений регламент використання ШІ.

Відмінно: Студент дав вичерпний та аргументований правовий аналіз порушень норм етики та процесуального права; точно розмежував цивільно-правову відповідальність LegalTech-сервісу та дисциплінарну відповідальність адвоката; розробив детальний та деталізований проєкт корпоративного регламенту використання ШІ.

Задовільно: Студент базово описав ситуацію без глибокого обґрунтування нормами законодавства про адвокатуру та захист даних, рішення містить лише поверхневі рекомендації щодо використання генеративних моделей.

Кейс 2. Захист «нейроправ» та когнітивної свободи при використанні імплантованих нейроінтерфейсів у трудових відносинах

ІТ-компанія «NeuroFuture» впровадила обов'язкове використання нейроінтерфейсу (Brain-Computer Interface, BCI) у формі гарнітури для своїх розробників та юридичних аналітиків з метою аналізу рівня концентрації, втоми та продуктивності. Колишній юрист компанії, після звільнення, виявив, що його нейродані (ЕЕГ-активність мозку, реакції на стимули, емоційні стани) не лише зберігалися на серверах компанії, але й були передані третій стороні — нейромаркетинговому агентству для дослідження «когнітивних паттернів ухвалення рішень». Юрист звернувся до суду з позовом про порушення його «нейроправ» (neurorights), ментальної приватності та когнітивної свободи, вимагаючи видалення даних та виплати моральної шкоди. Компанія

стверджує, що юрист підписав згоду на обробку даних при прийнятті на роботу.

Алгоритм обговорення:

Проаналізувати статус нейроданих (brain data) у системі законодавства про захист персональних даних (GDPR / Закон України «Про захист персональних даних») та віднести їх до відповідної категорії.

Дати правову оцінку концепції «нейроправ» (право на ментальну приватність, когнітивну свободу, ментальну недоторканність) у контексті міжнародно-правових стандартів прав людини (ст. 8 ЄКПЛ).

Оцінити правомірність згоди працівника на збір та передачу нейроданих у контексті дисбалансу сил у трудових відносинах.

Сформулювати розрахунок та обґрунтування позовних вимог щодо захисту ментальної приватності та компенсації моральної шкоди, завданої некоректною обробкою біометричних/нейронних даних.

Критерії оцінювання:

Добре: Студент правильно кваліфікував нейродані як чутливу категорію персональних даних та виявив порушення трудового/інформаційного права, проте концепцію нейроправ висвітлив лише на теоретичному рівні без чіткого прив'язування до судової практики.

Відмінно: Студент продемонстрував глибоке розуміння концепції нейроправ (neurorights), вдало інтегрував міжнародні стандарти прав людини та практики ЄСПЛ із вимогами GDPR, повністю спростував правомірність «згоди» у трудових відносинах та дав вичерпне вирішення спору.

Задовільно: Студент звів аналіз кейсу до загального спору про захист персональних даних, ігноруючи специфіку нейротехнологій, трансгуманістичного контексту та концепції когнітивної свободи.

Рекомендації для самостійної роботи

Під час опрацювання теми зосередьте увагу на моделях трансформації юридичного бізнесу (зокрема відході від традиційних білінгових годин) під впливом спеціалізованих LegalTech-асистентів на основі великих мовних моделей (Harvey, CoCounsel). Проаналізуйте концептуалізацію «нейроправ» (neurorights) та когнітивної свободи через призму адаптації трудового та цивільного законодавства до розвитку нейротехнологій і мозок-комп'ютерних інтерфейсів. Окремо вивчіть ризики витоку адвокатської таємниці, виникнення ШІ-галюцинацій та загрози квантових обчислень для постквантової криптографії та захисту даних.

Питання для самоконтролю:

Як використання спеціалізованих правових когнітивних асистентів (Harvey AI, CoCounsel) впливає на професійні стандарти належної обачності (due diligence) та етичні обов'язки адвоката щодо збереження адвокатської таємниці?

У чому полягає загроза розвитку квантових обчислень для сучасної постквантової криптографії та які правові механізми захисту критичної інформаційної інфраструктури мають бути впроваджені для нейтралізації цих ризиків?

Яким чином концепція «нейроправ» (neurorights) та захисту когнітивної свободи співвідноситься із чинними міжнародними стандартами прав людини в контексті використання імплантованих нейроінтерфейсів у трудових відносинах?

Завдання для самостійної роботи:

Проаналізуйте гіпотетичний кейс використання LegalTech-платформи на основі генеративного ШІ під час підготовки процесуальних документів, у результаті якого до тексту потрапили фальсифіковані судові прецеденти («галюцинації ШІ») та стався витік конфіденційних даних клієнта. Складіть юридичний висновок (Legal Memo) щодо етичної та дисциплінарної відповідальності адвоката, запропонувавши алгоритм перевірки фактів та профілактики таких ризиків.

Розробіть проєкт корпоративного Положення про захист нейроправ та когнітивної свободи працівників для підприємства, що планує впроваджувати нейроінтерфейси для моніторингу рівня концентрації та виснаження персоналу, враховуючи вимоги GDPR, етичні стандарти та норми трудового права.

YouTube, онлайн-курси та корисні ресурси

Офіційний сайт фундації захисту нейроправ NeuroRights Foundation - <https://neurorightsfoundation.org/>

Розділ стандартів постквантової криптографії на порталі NIST - <https://csrc.nist.gov/projects/post-quantum-cryptography>

Портал ЄС з цифрової стратегії та регулювання ШІ (European Commission - Digital Strategy) - <https://digital-strategy.ec.europa.eu/>

ПОЛІТИКА КУРСУ

1) щодо системи поточного і підсумкового контролю Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з “Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти”. Ознайомитись з документом можна за посиланням.	
2) щодо оскарження результатів контрольних заходів Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за посиланням.	
3) щодо відпрацювання пропущених занять Згідно “Положення про організацію освітнього процесу” здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом/робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥ 35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за посиланням.	
4) щодо дотримання академічної доброчесності “Положення про академічну доброчесність” закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за посиланням. Ознайомитись з “Політикою академічної доброчесності” - за посиланням.	
5) щодо використання штучного інтелекту “Положення про академічну доброчесність” визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за посиланням. “Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів” містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за посиланням.	

6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анулюється без права перескладання. Ознайомитись з відповідним документом можна за [посиланням](#).

Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.



7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за [посиланням](#).



№ п/п	Перелік сертифікованих (безкоштовних) онлайн-курсів	Перелік тем, які можуть бути перераховані (за умови наявності сертифіката на ім'я та прізвище студента/студентки)
1.	Від початківця до експерта в ШІ	Тема 1. Основи технології штучного інтелекту. Що і чому необхідно знати юристу
	AI For Everyone	Тема 2. Переваги та ризики використання ШІ. Оцінка ефективності використання ШІ
2.	ChatGPT Prompt Engineering for Developers	Тема 4. Генеративний ШІ та промпт-інжиніринг для юристів. Аналіз документів та даних за допомогою

Зміст самостійної роботи здобувачів
Розподіл годин, виділених на вивчення дисципліни:

Найменування видів робіт	Розподіл годин за формами навчання	
	денна	заочна
Самостійна робота, год, у т.ч.:	60	74
Опрацювання матеріалу, викладеного на лекціях	12	15
Підготовка до практичних занять та контрольних заходів	12	15
Підготовка звітів з практичних робіт	12	14
Підготовка до поточного контролю	12	15
Опрацювання матеріалу, винесеного на самостійне вивчення	12	15

МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання здобувачів вищої освіти з метою розвитку їхнього критичного, евристичного та алгоритмічного мислення, формування культури промпт-інжинірингу, здатності виявляти когнітивні й технічні ризики ШІ, забезпечувати етичний та нормативний комплаєнс у сфері LegalTech і готувати обґрунтовані магістерські правові рішення.

Програмний результат навчання	Метод навчання	Метод оцінювання
ПРН 3. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, цифрові, сучасні методи дослідження.	Проблемні лекції щодо архітектури великих мовних моделей (LLM), засад RAG-систем (Retrieval-Augmented Generation) та інструментів автоматизованої обробки неструктурованих правових даних; Лабораторний практикум: застосування генеративного ШІ (Advanced Data Analysis) для генерації та виконання Python/SQL-скриптів із метою парсингу, очищення та аналізу вивантажень судових рішень з ЄДРСР (кейс до теми 4); Метод структурованого контент-аналізу документів через Prompt Decomposition.	Оцінювання лабораторного звіту з парсингу та очищення масиву судових рішень (виконання та верифікація Python-коду); Комп'ютерний тестовий контроль у СДО Moodle на знання технічних та правових засад роботи RAG-систем і LLM;
ПРН 4. Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.	Метод кейс-стаді та судових симуляцій на основі знакових прецедентів: <i>State v. Loomis, Schufa (C-634/21), Mata v. Avianca</i> , справа Роберта Вільямса (Детройт); Семінарські дебати щодо меж «алгократії», концепції когнітивного суверенітету (Л. Байгрейв) та етичних викликів трансгуманізму і «нейроправ» (neurorights); Презентація групових проєктів: публічний захист розробленої концепції участі AI-стартапу в українській регуляторній пісочниці (Regulatory Sandbox) або аудиту системи Amsterdam Smart Check.	Оцінювання усних доповідей, презентацій та аргументації під час розбору кейсів на практичних заняттях; Експертна оцінка якості підготовленої аналітичної доповіді/виступу щодо допустимості систем оцінки рецидивізму (COMPAS) у судах; Взаємне рецензування (peer-review) виступів та аргументації опонентів у навчальних дебатах.
ПРН 8. Оцінювати достовірність інформації	Практикум із верифікації вихідних даних: алгоритми	Перевірка розробленого студентом алгоритму

та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.	виявлення галюцинацій моделей, фактчекінг цитат і реквізитів справ у ЄДРСР (кейс «Фантомний прецедент та витік даних»); Метод критичного промптингу: реалізація фреймворків <i>Chain-of-Verification (CoVe)</i> та <i>Chain-of-Thought (CoT)</i> для багаторівневої самоперевірки ШІ; Застосування методології <i>анти-анкерингу</i> (формування власних гіпотез до звернення до моделі) та «тесту на спрощення» для подолання ефекту планаризації й дескілінгу.	верифікації (Fact-Checking Framework) для перевірки згенерованих ШІ текстів; Оцінювання якості виявлення штучних «галюцинацій» та помилок у змодельованих процесуальних документах.
ПРН 9. Генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.	Тренінг із промпт-інжинірингу: фреймворк «Персона → Контекст → Проблема», Few-Shot Prompting, задання явних обмежень (negative constraints); Проектування локальних регламентів (AI Use Policy, SOP) для юридичних фірм щодо безпечного використання GenAI та запобігання <i>input problem</i> (витоку таємниці); Моделювання LegalTech-рішень: розрахунок ROI та бізнес-метрик автоматизації договірної роботи (contract review) Розробка архітектури системи «Human-in-the-Loop» для комплаєнсу з вимогами ст. 22 GDPR та класифікації систем високого ризику за EU AI Act.	Оцінювання створених структурованих Few-Shot та CoVe-промптів під час виконання лабораторних завдань; Експертиза підготовленого проекту корпоративного регламенту (SOP) адвокатського об'єднання щодо використання ШІ та захисту конфіденційності; Оцінювання розробленої матриці комплаєнсу та розрахунку ROI впровадження LegalTech-інструменту в юридичний департамент.
ПРН17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності	Комплексний міждисциплінарний аналіз та розв'язання прикладних правових казусів (case-study) у ключових галузях права: – у приватно-правовій сфері: розв'язання спорів щодо	Оцінювання підготовлених проєктів галузевих процесуальних документів та аналітичних висновків: – проєкту резолютивної частини судового рішення щодо розподілу цивільно-

	волевиявлення, помилки правочину та деліктної відповідальності при алгоритмічних збоях автономних ІІІ-агентів у смарт-контрактах; кваліфікація порушень авторського права на AI-контент і меж режиму Text and Data Mining (Тема 6); – у публічно-правовій сфері: правова оцінка рішень автоматизованого скорингу, моніторингу виплат і захисту прав вразливих груп крізь призму ст. 22 GDPR, концепції Due Process та практики Суду ЄС (Schufa C-634/21, MiDAS) (Тема 5); – у сфері кримінальної юстиції: вирішення процесуальних колізій щодо допустимості цифрових доказів мультимодальних платформ (Longeye) у світлі ст. 6 ЄКПЛ та проблеми «чорної скриньки» (State v. Loomis) (Тема 7); •	правової відповідальності за збитки від збою автономного ІІІ-агента (кейс 2 теми 6); – звернення/скарги на підставі ст. 22 GDPR щодо незаконного автоматизованого профайлінгу й відмови у банківському кредитуванні (кейс 1 теми 6); – ухвали слідчого судді/суду щодо оцінки допустимості доказів, отриманих за допомогою ІІІ-систем (кейс 1 теми 7)
--	--	--

МАТЕРІАЛЬНО-ТЕХНІЧНІ РЕСУРСИ

Мультимедійне обладнання для проведення лекцій і презентацій; доступ до аналітичних платформ CrimeDataLab та IFSafeLab; доступ до Єдиного державного реєстру судових рішень та порталу відкритих даних; хмарне сховище для ведення наскрізного проєкту (Google Disk UKD); система дистанційного навчання Moodle.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Контрольні заходи

Вид	Зміст	% від загальної оцінки	Бал	
			min	max
Поточні контрольні заходи	Фронтальні опитування, оцінювання доповідей під час запланованих дискусій	60	35	60
Підсумкові контрольні заходи	Тестування	40	25	40
Всього:		100	60	100

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів».

Фіксація **поточного** контролю здійснюється в “Електронному журналі обліку успішності академічної групи” на підставі чотирибальної шкали - “2”; “3”; “4”; “5”. У разі відсутності студента на занятті виставляється “н”. За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість “н” в журналі буде виставлено “0” (нуль балів), без права

перездачі. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».²

Критерії оцінювання³ (поточного та підсумкового контролю)

До підсумкового контролю допускаються студенти які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (диференційований залік/екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно з **Шкалою оцінювання знань за ЄКТС**) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС:

Оцінка за національною шкалою	Рівень досягнень, %	Шкала ECTS
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B
	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з'явилися на заліки/екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

² можна вказати теми чи завдання, які є обов'язковими до виконання, а також особисті підходи до оцінювання рівня знань здобувачів під час аудиторної роботи

³ критерії вказуються згідно з особливостями дисципліни.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Karchevskiy, M., Losych, S., & Germanov, S. (2023). Socialization of artificial intelligence and transhumanism: legal and economic aspects. *Baltic Journal of Economic Studies*, 9(1), 61-70. <https://doi.org/10.30525/2256-0742/2023-9-1-61-70>
2. Karchevskiy M., Radutniy O. Ukrainian report on traditional criminal law categories and AI. *Revue Internationale de Droit Penal*. 2023. Vol. 2023. P. 363–383.
3. Karchevskiy M., Radutniy O. Ukrainian report on criminalisation of AI-related offences. *Revue Internationale de Droit Penal*. Vol. 95 issue I, 2024. P. 383–406.
4. Карчевський М.В. Розділ 5. Обчислювальне кримінологічне аргументування та його роль в раціоналізації кримінально-правової правотворчості // Концептуальні засади правотворчості у сфері кримінальної юстиції : монографія / за ред. д. ю. н., проф. Зої Загиней-Заболотенко. Київ : Юрінком Інтер, Інститут держави і права імені В. М. Корецького НАН України, 2025. С. 222-272
5. Карчевський М. В. Кримінальне право в умовах цифрової трансформації. Від несанкціонованого доступу до «jailbreak» штучного інтелекту : монографія / Микола Карчевський ; Ун-т Короля Данила ; Ін-т інформації, безпеки і права Нац. акад. прав. наук України. – Харків : Право, 2025. – 176 с.
6. Карчевський, М. В., & Карчевська, О. В. (2025). Структурний вимір правового регулювання ШІ. *Український політико-правовий дискурс*, (12). <https://doi.org/10.5281/zenodo.15782211>
7. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В. С. Батиргарєєва (голов. ред.) та ін. Харків: Право. 2023. Вип. 46. С. 21-31. <http://pbz.nlu.edu.ua/article/view/301290/293453>
8. Карчевський М. В. Перспективи правового регулювання в контексті гіпотези розвитку технологій трансгуманізму. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2019. № 1(85), С. 115-127.

Тема 1. Основи технології штучного інтелекту. Що і чому необхідно знати юристу

1. Сучасні тенденції цифрової трансформації юриспруденції та LegalTech / О. В. Харитонова, Є. О. Харитонов // Часопис цивілістики. 2023. Вип. 48. С. 12–19. URL: <http://chasopyscivilystyky.onu.edu.ua/archive/48/3.pdf> .

2. Tomorrow's Lawyers: An Introduction to Your Future / R. Susskind // Oxford University Press. 2023. URL: <https://global.oup.com/academic/product/tomorrow-lawyers-9780192867018> .
3. Model Rules of Professional Conduct: Rule 1.1 Competence / American Bar Association // ABA Center for Professional Responsibility. 2023. URL: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/ .
4. Legal Tech and the Future of Legal Services / M. Hartung, M. Bues, G. Halbleib // European Journal of Law and Technology. 2022. Vol. 13. No. 2. URL: <https://ejlt.org/index.php/ejlt/article/view/845> .
5. AI competency framework for students / UNESCO // UNESCO Publishing. 2024. 64 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000391104> .
6. OECD Digital Education Outlook 2023: Towards an Educational Health Check / OECD // OECD Publishing. 2023. URL: <https://www.oecd.org/education/digital-education-outlook/> .
7. Ethics of Artificial Intelligence and the Human-in-the-Loop Principle in Judicial Decision-Making / G. Sartor // European University Institute Working Papers. 2023. URL: <https://cadmus.eui.eu/handle/1814/75421> .
8. Штучний інтелект у правовому полі: поняття, класифікація та перспективи правового регулювання / І. В. Дячук // Право та інновації. 2023. № 2 (42). С. 35–42. URL: [https://doi.org/10.37772/2518-7171-2023-2\(42\)-5](https://doi.org/10.37772/2518-7171-2023-2(42)-5) .
9. Deep Learning for Legal Text Processing: A Survey / A. Zablocki et al. // Artificial Intelligence and Law. 2023. Vol. 31. P. 145–182. URL: <https://link.springer.com/article/10.1007/s10506-022-09322-1> .
10. Attention Is All You Need / A. Vaswani, N. Shazeer, N. Parmar et al. // Advances in Neural Information Processing Systems (NeurIPS 2017). 2017. Vol. 30. URL: <https://arxiv.org/abs/1706.03762> .
11. Law and Large Language Models: A Guide to AI Prompting, Technologies, and Applications / P. Henderson et al. // arXiv Preprint. 2023. URL: <https://arxiv.org/abs/2303.07134> .
12. Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models / M. Dahl et al. // Stanford University Research Paper. 2024. URL: <https://law.stanford.edu/publications/large-legal-fictions-profiling-legal-hallucinations-in-large-language-models/> .
13. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> .
14. AI-Driven Legal Analytics and Contract Review Automation / J. Armour, H. P. Pargendler // Harvard Business Law Review. 2023. Vol. 13. P. 201–245. URL: <https://www.hblr.org/volume-13-articles/> .
15. Predictive Analytics in the Judicial System: Ethical Constraints and Accuracy Standards / K. Ashley // Legal Information Science. 2022. Vol. 40. P. 99–120. URL: <https://doi.org/10.1007/s10506-022-09311-2> .

16. Mata v. Avianca, Inc., No. 1:22-cv-01461 (S.D.N.Y. June 22, 2023) // CourtListener. 2023. URL: <https://www.courtlistener.com/docket/63107798/mata-v-avianca-inc/> .
17. State v. Loomis, 881 N.W.2d 749 (Wis. 2016) // Justia Law. 2016. URL: <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html> .
18. Thomson Reuters Enterprise Centre GmbH v. ROSS Intelligence Inc., No. 1:20-cv-00613 (D. Del. 2023) // CourtListener. 2023. URL: <https://www.courtlistener.com/docket/17130081/thomson-reuters-enterprise-centre-gmbh-v-ross-intelligence-inc/> .

Тема 2. Переваги та ризики використання ШІ. Оцінка ефективності використання ШІ

1. Регламент Європейського Парламенту і Ради (ЄС) 2024/1689 про встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) / Європейський Союз // Офіційний вісник ЄС. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> .
2. Рекомендація щодо етики штучного інтелекту / ЮНЕСКО // Офіційний портал ЮНЕСКО. 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137_ukr .
3. A Hallucination-Free Legal LLM? Assessing the Reliability of Generative AI in Legal Research / D. Dahl, V. Guha, A. Ho et al. // Stanford Institute for Human-Centered AI (HAI). 2024. URL: <https://hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models> .
4. ABA Formal Opinion 512: Generative Artificial Intelligence Tools / American Bar Association // ABA Standing Committee on Ethics and Professional Responsibility. 2024. URL: <https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-ethics-opinion-ai-tools/> .
5. Judicial Order on Sanctions in Roberto Mata v. Avianca, Inc. (Case No. 22-cv-1461) / United States District Court, S.D. New York // CourtListener. 2023. URL: <https://www.courtlistener.com/docket/63107798/54/mata-v-avianca-inc/> .
6. State v. Loomis (881 N.W.2d 749 (Wis. 2016)) / Supreme Court of Wisconsin // Harvard Law Review. 2017. URL: <https://harvardlawreview.org/print/vol-130/state-v-loomis/> .
7. CCBE Guidance on the Use of Artificial Intelligence by Lawyers and Law Firms / Council of Bars and Law Societies of Europe // CCBE Portal. 2023. URL: https://www.ccbe.eu/NWG/portal/page/portal/CCBE/uploads/pdf/CCBE_CoE/2023/CCBE-Guidance-on-AI.pdf .
8. Decision Moffatt v. Air Canada (2024 BCCRT 149) / Civil Resolution Tribunal of British Columbia // CanLII. 2024. URL: <https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149/2024bccrt149.html> .

**Тема 3. Правове регулювання ШІ. Досвід ЄС, США та Китаю.
Регулювання ШІ в Україні**

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // EUR-Lex. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> .
2. Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence / The White House // The Federal Register. 2023. URL: <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> .
3. Interim Measures for the Management of Generative Artificial Intelligence Services / Cyberspace Administration of China // DigiChina (Stanford University translation). 2023. URL: <https://digichina.stanford.edu/work/translation-interim-measures-for-the-management-of-generative-artificial-intelligence-services/> .
4. Дорожня карта з регулювання штучного інтелекту в Україні / Міністерство цифрової трансформації України // Офіційний вебпортал Мінци2023. [фри](https://thedigital.gov.ua/news/mintsifra-%D0%BF%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D1%83%D0%B2%D0%B0%D0%BB%D0%B0-%D0%B4%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8E-%D0%BA%D0%B0%D1%80%D1%82%D1%83-%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE-%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83-%D0%B2-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96). URL: <https://thedigital.gov.ua/news/mintsifra-%D0%BF%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D1%83%D0%B2%D0%B0%D0%BB%D0%B0-%D0%B4%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8E-%D0%BA%D0%B0%D1%80%D1%82%D1%83-%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE-%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83-%D0%B2-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96> .
5. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX // Офіційний вебпортал Верховної Ради України. 2022. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text> .
6. Regulatory Sandboxes and Other Exploratory Approaches to AI Governance / Organisation for Economic Co-operation and Development // OECD iLibrary. 2023. URL: <https://doi.org/10.1787/471694f2-en> .
7. NJCM c.s./De Staat der Nederlanden (SyRI) : Judgment of the District Court of The Hague / Rechtspraak.nl. 2020. URL: <https://uitspraken.rechtspraak.nl/soort/rechtspraak/details?id=ECLI:NL:RBDHA:2020:1878> .
8. Stephen Thaler v. Kathi Vidal : Decision of the U.S. Court of Appeals for the Federal Circuit (No. 2021-2347) // U.S. Court of Appeals for the Federal Circuit. 2022. URL: https://www.cafc.uscourts.gov/opinions-orders/21-2347.OPINION.8-5-2022_1988142.pdf .

Тема 4. Генеративний ШІ та промпт-інжиніринг для юристів.
Аналіз документів та даних за допомогою ШІ

1. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX // Офіційний вебпортал парламенту України. 2022. URL: <https://zakon.rada.gov.ua/laws/show/2811-20> .
2. OECD Artificial Intelligence Review : Recommendation of the Council on Artificial Intelligence // OECD Legal Instruments. 2019. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> .
3. Recommendation on the Ethics of Artificial Intelligence // UNESCO Digital Library. 2021. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> .
4. Thinking, Fast and Slow / Kahneman D. New York : Farrar, Straus and Giroux, 2011. 512 p. URL: https://www.google.com/books/edition/Thinking_Fast_and_Slow/Z-A_DwAAQBAJ .
5. A Prompt Pattern Language for Large Language Models / White J., Fu Q., Hays S. et al. // arXiv preprint arXiv:2302.11382. 2023. URL: <https://arxiv.org/abs/2302.11382> .
6. Online Courts and the Future of Justice / Susskind R. Oxford : Oxford University Press, 2019. 368 p. URL: <https://global.oup.com/academic/product/online-courts-and-the-future-of-justice-9780198838364> .
7. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models / Wei J., Wang X., Schuurmans D. et al. // Advances in Neural Information Processing Systems (NeurIPS). 2022. URL: <https://arxiv.org/abs/2201.11903> .
8. Language Models are Few-Shot Learners / Brown T. B., Mann B., Ryder N. et al. // arXiv preprint arXiv:2005.14165. 2020. URL: <https://arxiv.org/abs/2005.14165> .
9. Chain-of-Verification Reduces Hallucination in Large Language Models / Dhuliawala S., Komeili M., Xu J. et al. // arXiv preprint arXiv:2309.11495. 2023. URL: <https://arxiv.org/abs/2309.11495> .
10. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks / Lewis P., Perez E., Piktus A. et al. // Advances in Neural Information Processing Systems. 2020. URL: <https://arxiv.org/abs/2005.11401> .
11. Retrieval-Augmented Generation for AI-Generated Content: A Survey / Yu H., Gan W., Chen L. et al. // arXiv preprint arXiv:2402.19473. 2024. URL: <https://arxiv.org/abs/2402.19473> .
12. Про судоустрій і статус суддів : Закон України від 02.06.2016 № 1402-VIII // Офіційний вебпортал парламенту України. 2016. URL: <https://zakon.rada.gov.ua/laws/show/1402-19> .
13. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age / Ashley K. D. Cambridge : Cambridge University Press, 2017. 426 p. URL: <https://doi.org/10.1017/9781316756478> .
14. Правила адвокатської етики : затверджені Звітно-виборним з'їздом адвокатів України 09.06.2017 р. // Національна асоціація адвокатів України. 2017. URL: <https://unba.org.ua/pravyla-advokatskoi-etyky.html> .

15. Smart Technologies and the End of Law: Something Is Happening Here / Hildebrandt M. Cheltenham : Edward Elgar Publishing, 2015. 304 p. URL: <https://www.e-elgar.com/shop/gbp/smart-technologies-and-the-end-of-law-9781782549482.html> .
16. Artificial Intelligence and Law: An Overview / Surden H. // Georgia State University Law Review. 2019. Vol. 35, No. 4. P. 1305–1337. URL: <https://doi.org/10.2139/ssrn.3411449> .
17. Європейська етична хартія про використання штучного інтелекту в судових системах та їхньому оточенні // Рада Європи (СЕПЕJ). 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> .
18. Roberto Mata v. Avianca, Inc. : Memorandum Opinion and Order of US District Court, S.D. New York, June 22, 2023. No. 22-cv-1461 (PKC) // CourtListener. 2023. URL: <https://www.courtlistener.com/docket/63313426/mata-v-avianca-inc/> .
19. Park v. Kim : Opinion of US Court of Appeals for the Second Circuit, Jan 29, 2024. No. 22-2057 // US Court of Appeals for the Second Circuit. 2024. URL: <https://www.ca2.uscourts.gov/decisions> .
20. Ухвала Дніпропетровського окружного адміністративного суду від 16.10.2023 у справі № 160/27582/23 // Єдиний державний реєстр судових рішень. 2023. URL: <https://reyestr.court.gov.ua/Review/114210081> .

Тема 5. Штучний інтелект у державному управлінні та електронному урядуванні

1. Алгоритмічне врядування та права людини у цифрову еру / ред. О. В. Баранов // Інститут держави і права ім. В. М. Корецького НАН України. 2024. URL: <https://idp.org.ua/publications/algorithmic-governance-2024>.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) // EUR-Lex. 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> .
3. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 / European Data Protection Board // EDPB Official Website. 2018. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-automated-individual-decision-making-and-profiling-purposes_en .
4. Ethics Guidelines for Trustworthy AI / High-Level Expert Group on AI // European Commission. 2019. URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> .
5. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation / S. Wachter, B. Mittelstadt, L. Floridi // International Data Privacy Law. 2017. Vol. 7, No. 2. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 .
6. Data Protection Law: Approaching Its Rationale, Logic and Limits / L. A. Bygrave // Information Law Series, Kluwer Law International. 2014. URL: <https://kluwerlawonline.com/titleinfo/chapter/2014022> .

7. Algorithmic Accountability in Public Administration / UNESCO // UNESCO Digital Library. 2023. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000384120> .
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // EUR-Lex. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> .
9. Digital Omnibus Package: Regulatory Simplification and Fundamental Rights Protection / European Parliamentary Research Service // European Parliament Think Tank. 2025. URL: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)768012](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)768012) .
10. Governing with Artificial Intelligence: Are Public Administrations Ready? / OECD // OECD Public Governance Reviews. 2025. URL: https://www.oecd-ilibrary.org/governance/governing-with-artificial-intelligence_868f0e0b-en .
11. Bauserman v. Michigan Unemployment Insurance Agency, No. 160813 / Michigan Supreme Court // Michigan State Courts Official Portal. 2022. URL: https://www.courts.michigan.gov/siteassets/case-documents/opinions/final/sc/160813_76_01.pdf .
12. Amsterdam Smart Check Case Study: Lessons on Algorithmic Bias in Welfare Governance / City of Amsterdam Audit Office // Algorithm Register of Amsterdam. 2023. URL: <https://algoritmeregister.amsterdam.nl/en/smart-check-welfare> .
13. Judgment of the Court (Grand Chamber) in Case C-634/21 (SCHUFA Holding AG) // InfoCuria - Case-law of the Court of Justice. 2023. URL: <https://curia.europa.eu/juris/liste.jsf?num=C-634/21> .
14. Brazilian City Passes Law Written Entirely by ChatGPT / Associated Press News. 2023. URL: <https://apnews.com/article/brazil-chatgpt-law-porto-alegre-f39b1a547798361005f25a918a5f822a> .
15. Algocracy and the Problem of Democratic Legitimacy / A. Ferdman // Political Theory. 2022. URL: <https://journals.sagepub.com/doi/10.1177/00905917221102934> .
16. Legal Analysis of the SyRI Judgment by the District Court of The Hague / Netherlands Commission for Human Rights. 2020. URL: <https://mensenrechten.nl/nl/publicatie/syri-judgment-analysis-2020> .

Тема 6. Приватно-правовий контекст III. Право не бути суб'єктом автоматизованих рішень. Автоматизація договірної роботи. Авторське право та III

1. 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) / European Parliament, Council of the European Union // EUR-Lex. 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> (дата звернення: 24.10.2023).

2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) / European Parliament, Council of the European Union // EUR-Lex. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 15.07.2024).
3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) / European Parliament // European Parliament. 2017. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата звернення: 10.11.2023).
4. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV / Верховна Рада України // Законодавство України. 2003. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 01.09.2024).
5. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX / Верховна Рада України // Законодавство України. 2022. URL: <https://zakon.rada.gov.ua/laws/show/2811-20> (дата звернення: 01.09.2024).
6. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market / European Parliament, Council of the European Union // EUR-Lex. 2019. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790> (дата звернення: 12.02.2024).
7. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence / US Copyright Office, Library of Congress // Copyright.gov. 2023. URL: https://www.copyright.gov/ai/ai_policy_guidance.pdf (дата звернення: 05.05.2024).
8. Court of Appeal of Amsterdam, Uber drivers automated decision-making judgment (Case 200.295.747/01, ECLI:NL:GHAMS:2023:793) / Court of Appeal of Amsterdam // Rechtspraak.nl. 2023. URL: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793> (дата звернення: 18.01.2024).

Тема 7. ШІ та кримінально-правове регулювання. Використання ШІ для вчинення злочинів. ШІ в діяльності правоохоронних органів та судів

1. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement / A. G. Ferguson // Google Books. 2017. URL: https://books.google.com/books?id=U_E3DwAAQBAJ.
2. Artificial Intelligence and Policing: A Primer for Law Enforcement Leadership / Police Executive Research Forum // National Institute of Justice. 2021. URL: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/artificial-intelligence-and-policing-primer-law-enforcement>.
3. Big Data and Policing: An Assessment of Law Enforcement Analytics in the UK / A. Babuta // Royal United Services Institute (RUSI). 2018. URL: <https://rusi.org/explore-our-research/publications/occasional-papers/big-data-and-policing>.

4. Avon and Somerset Police test AI tool 'Soze' to solve cold cases / BBC News // BBC. 2024. URL: <https://www.bbc.com/news/articles/c1e52847248o> .
5. To predict and serve? / K. Lum, W. Isaac // HRDAG Research. 2016. URL: <https://hrdag.org/publications/to-predict-and-serve/> .
6. Santa Cruz becomes first U.S. city to ban predictive policing / Reuters // Reuters. 2020. URL: <https://www.reuters.com/article/us-usa-tech-police-trfn-idUSKBN23V2ZP> .
7. Algorithmic Risk Assessment in Police Custody: Durham Constabulary's HART System / H. Urwin // University of Cambridge Institute of Criminology. 2021. URL: <https://www.crim.cam.ac.uk/research/hart-system-evaluation> .
8. Robert Williams v. City of Detroit: Settlement Agreement and Facial Recognition Policy Changes / ACLU Michigan // ACLU. 2024. URL: <https://www.aclumich.org/en/press-releases/aclu-settlement-detroit-police-department-establishes-nationwide-model-limit> .
9. Body-Worn Cameras and Artificial Intelligence in Policing / Police Executive Research Forum // PERF. 2021. URL: <https://www.policeforum.org/bwc-ai-report> .
10. State v. Loomis, 881 N.W.2d 749 (Wis. 2016) // Harvard Law Review. 2017. URL: <https://harvardlawreview.org/print/vol-130/state-v-loomis/> .
11. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) // EUR-Lex. 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> .
12. Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act) // EUR-Lex. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> .

***Тема 8. Професійна юридична діяльність та розвиток технологій.
LegalTech проєкти на основі ШІ. Правове регулювання квантових
обчислень та технологій трансгуманізму***

1. Generative AI in the Legal Sector / Artificial Lawyer // Artificial Lawyer. 2023. URL: <https://www.artificiallawyer.com/category/generative-ai/> .
2. Allen & Overy announces unprecedented firm-wide partnership with Harvey / Allen & Overy Press Release // A&O Shearman. 2023. URL: <https://www.aoshearman.com/en/news-and-insights/news/allen-and-overly-announces-unprecedented-firm-wide-partnership-with-harvey>
3. CoCounsel AI Legal Assistant / Thomson Reuters // Thomson Reuters Legal Solutions. 2023. URL: <https://legal.thomsonreuters.com/en/products/cocounsel>
4. Future of Legal Services and AI Impact Report / OECD // OECD iLibrary. 2022. URL: <https://www.oecd.org/en/topics/sub-issues/ai-governance-and-ethics.html>
5. Report on Post-Quantum Cryptography / National Institute of Standards and Technology // NIST CSRC. 2022. URL: <https://csrc.nist.gov/publications/detail/nistir/8413/final>

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI / Верховна Рада України // Офіційний вебпортал парламенту України. 2010. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
7. Post-Quantum Cryptography Standardization / ENISA // European Union Agency for Cybersecurity. 2023. URL: <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>
8. Recommendation on the Ethics of Neurotechnology / UNESCO // UNESCO Digital Library. 2023. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000385728>
9. Four ethical priorities for neurotechnologies and AI / Yuste R., Goering S. et al. // Nature. 2017. URL: <https://www.nature.com/articles/551159a> (дата звернення: 10.11.2023).
10. Law on Protection of Neurodata and Neurorights in Chile / Senate of Chile // BCN Law Library. 2021. URL: <https://www.bcn.cl/leychile/navegar?idNorma=1166983>
11. Model Rules of Professional Conduct: Rule 1.1 Competence / American Bar Association // ABA Center for Professional Responsibility. 2020. URL: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/ (дата звернення: 02.11.2023).
12. Правила адвокатської етики : затверджені Звітно-виборним з'їздом адвокатів України 09.06.2017 року / Національна асоціація адвокатів України // Офіційний сайт НААУ. 2017. URL: <https://unba.org.ua/assets/uploads/legislations/pravyla/2017-06-09-pravyla-advokatskoi-etyky.pdf>
13. CCBE Guidance on the Use of Artificial Intelligence by Lawyers and Law Firms / Council of Bars and Law Societies of Europe (CCBE) // CCBE Publications. 2023. URL: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_2023_CCBE_Guidance_AI.pdf
14. Judicial Guidance on the Use of AI / Courts and Tribunals Judiciary of England and Wales // UK Judiciary. 2023. URL: <https://www.judiciary.uk/guidance-and-resources/artificial-intelligence-ai-judicial-guidance/> .
15. Roberto Mata v. Avianca, Inc. : Order Imposing Sanctions, No. 22-cv-1461 (S.D.N.Y. June 22, 2023) / Castel P. K. // CourtListener. 2023. URL: <https://www.courtlistener.com/docket/63107798/mata-v-avianca-inc/>
16. Girardi v. Emotiv Inc. : Ruling on Neurorights Protection, Rol No. 105.892-2022 / Supreme Court of Chile // Poder Judicial de Chile. 2023. URL: <https://www.pjud.cl/prensa-y-comunicaciones/noticias-del-poder-judicial/96645>
17. State v. Loomis : 881 N.W.2d 749 (Wis. 2016) / Supreme Court of Wisconsin // Harvard Law Review. 2016. URL: <https://harvardlawreview.org/print/vol-130/state-v-loomis/>

