МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Кафедра кримінального процесу і криміналістики

«ЗАТВЕРДЖУЮ»
Проректор
з науково-педагогічної роботи
та міжнародної співпраці
Львівського національного університету
імені Івана Франка
проф. Різник С. В.

_____

«___»_____2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки»

Галузь знань: **12 «Інформаційні технології»**
Спеціальність: **125 «Кібербезпека»**
вибіркова навчальна дисципліна

Юридичний факультет

Львів – 2024 рік

Робоча програма навчальної дисципліни «Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки» для студентів за галуззю знань *12 інформаційні технології*, спеціальністю *125 кібербезпека* у межах освітньо-професійної програми ОС бакалавр, 2024. 20 с.

Розробник:
Мурадов Валентин Валентинович, кандидат юридичних наук, доцент кафедри кримінального процесу і криміналістики

Робоча програма затверджена на засіданні кафедри кримінального процесу і криміналістики юридичного факультету Львівського національного університету імені Івана Франка (Протокол від « » 2024 року № 1)

Завідувач кафедри
кримінального процесу і криміналістики _____ Н. Р. Бобечко
« » 2024 року

Схвалено Вченою Радою юридичного факультету Львівського національного університету імені Івана Франка. Протокол від « » 2024 року № .

« » 2024 року Голова_____проф. В. М. Бурдін

© Мурадов В.В., 2024 рік

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>Денна форма навчання</th><th>Заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 4</td><td>Галузь знань 12 «Інформаційні технології»</td><td colspan="2">Вибіркова навчальна дисципліна</td></tr>
<tr><td rowspan="3">Спеціальність 125 «Кібербезпека»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>4</td><td>–</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td colspan="2">Семестр</td></tr>
<tr><td>8-й</td><td>–</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: аудиторних – 3 Самостійної роботи студента – 4,5</td><td rowspan="10">Освітньо-професійна програма ОС Бакалавр</td><td colspan="2">Лекцій</td></tr>
<tr><td>16</td><td>–</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>72</td><td>–</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить для денної форми навчання – 2:3.

Мова навчання: українська

2. МЕТА І ЗАВДАННЯ ДИСЦИПЛІНИ

Предмет. Перші роботи в галузі штучного інтелекту були проведені в 1950-х роках. У цей період були розроблені перші програмні системи, які могли виконувати деякі завдання, які раніше вважалися виключно людськими. У 1960-х роках інтерес до штучного інтелекту знизився, оскільки було виявлено, що розробка штучного інтелекту є більш складним завданням, ніж передбачалося. Однак у 1970-х роках інтерес до штучного інтелекту знову зріс. У цей період були розроблені нові підходи до штучного інтелекту, такі як нейронні мережі та експертні системи. У 1980-х роках штучний інтелект став більш практичним. У цей період були розроблені перші комерційні продукти, які використовували штучний інтелект, такі як системи розпізнавання голосу та штучного зору. У 1990-х роках штучний інтелект став ще більш потужним. У цей період були розроблені нові технології, такі як машинне навчання та штучний інтелект у реальному часі.

У 2000-х роках штучний інтелект став все більш поширеним. У цей період штучний інтелект використовувався в широкому спектрі застосувань, таких як автономні транспортні засоби, медична діагностика та кібербезпека.У 2010-х роках штучний інтелект став ще більш потужним і всеосяжним. У цей період були розроблені нові технології, такі як глибоке навчання (самонавчання) та квантовий тип компютерів.

Сьогодні штучний інтелект є однією з найважливіших технологій у світі. Він має потенціал для радикального зміни нашого життя в багатьох сферах, таких як робота, освіта, медицина та суспільство.Однак штучний інтелект також несе в собі ряд ризиків. Одним з найважливіших ризиків є можливість того, що штучний інтелект може стати надто потужним і небезпечним. Іншим ризиком є можливість того, що штучний інтелект може бути використаний для дискримінації та інших форм несправедливості. З цих причин важливо вивчати соціальні, етичні та правові аспекти штучного інтелекту. Це допоможе нам розробити штучний інтелект, який є безпечним, справедливим та корисним для суспільства.

Спецкурс "Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки" є важливою частиною цих зусиль. Він вивчає широкий спектр питань, пов'язаних з штучним інтелектом, його практичне використання та значні потенційні ризики, пов’язані з таким використанням

Мета спецкурсу: Штучний інтелект (ШІ) та кібербезпека є одними з найважливіших технологій сучасності, які мають значний вплив на наше суспільство. Розвиток цих технологій супроводжується низкою соціальних, етичних та правових проблем, які необхідно вирішувати. Мета спецкурсу "Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки" полягає в тому, щоб ознайомити студентів із цими проблемами та сприяти їхньому розумінню. Курс охоплює такі теми, як: соціальні наслідки ШІ та кібербезпеки: вплив цих технологій на суспільство, економіку, робочі місця, демократію тощо; етичні аспекти ШІ та кібербезпеки: питання справедливості, дискримінації, автономії, безпеки тощо; правові аспекти ШІ та кібербезпеки: законодавчий регулювання цих технологій, міжнародне співробітництво тощо. Курс допоможе студентам краще зрозуміти ці технології та їхній вплив на наше суспільство обговорити актуальні проблеми ШІ та кібербезпеки, а також розробити власні пропозиції щодо їхнього вирішення.

У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:

знати:

- чинне законодавство та нормативні акти, що регулюють ШІ, кібербезпеку та захист даних;
- методи та практики кібербезпеки, які можна використовувати для захисту систем ШІ;
- загрози та ризики їх функціонування та використання;
- економічні, соціальні та інші наслідки розвитку ШІ;
- принципи етики штучного інтелекту;
- основні напрями використання ШІ та кібербезпеки на службі суду та органів правопорядку.

вміти:

- аналізувати аргументи та робити обґрунтовані висновки щодо ШІ;
- застосовувати етичні принципи до прийняття рішень щодо розробки та використання ШІ;
- аналізувати правові наслідки рішень щодо розробки та використання ШІ;
- оцінювати соціальні наслідки рішень щодо розробки та використання ШІ;
- застосовувати принципи кібербезпеки до розробки та використання ШІ.

Необхідні попередні та супутні навчальні дисципліни: «Основи алгоритмізації та програмування», «Комп'ютерні мережі», «Комплексні системи захисту інформації».

3. КАР'ЄРНІ МОЖЛИВОСТІ

Кар'єрні перспективи. Випускники курсу можуть знайти себе як кваліфіковані кадри в галузі використання методів штучного інтелекту в органах державної влади та місцевого самоврядування, на підприємствах, установах, організаціях незалежно від форми власності. Вони можуть також працевлаштуватися як розробники програмного забезпечення елементів, оболонок та окремих версій штучного інтелекту. Також цей курс допоможе у подальших можливостях дослідження не лише вивчених аспектів штучного інтелекту та кібербезпеки, а й прогнозованих його форм і відгалужень. Цей курс також може використовуватися як доповнення (підвищення) кваліфікації для кар'єри у юридичних професіях у сферах розслідування і судочинства. Його цільовою аудиторією можуть бути й журналісти-розслідувачі та ІТ-аналітики.

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. **Вступ до штучного інтелекту та кібербезпеки**

Вступ

Що таке штучний інтелект (ШІ)? Короткий огляд історії ШІ. Різні галузі ШІ. Вплив ШІ на суспільство.

Кібербезпека.

Що таке кібербезпека? Різні типи кіберзагроз. Як кібербезпека пов'язана з ШІ.

ШІ та кібербезпека: можливості

Як ШІ може використовуватися для покращення кібербезпеки. Автоматизація аналізу даних. Виявлення аномалій. Прогнозування кібератак

ШІ та кібербезпека: ризики

Зловживання ШІ для кібератак. Створення більш складних кіберзагроз

Вразливість систем ШІ.

Тема 2. **Соціальні аспекти штучного інтелекту**

Вплив ШІ на ринок праці

Автоматизація та зникнення робочих місць. Створення нових робочих

місць, пов'язаних з ШІ. Перекваліфікація та підвищення кваліфікації робочої сили

ШІ та аспекти соціального управління

Вплив ШІ на прийняття рішень. Прозорість алгоритмів ШІ. Маніпулювання громадською думкою за допомогою ШІ.

Прогнозоіваність розвитку ШІ

Можливі сценарії розвитку ШІ. Вплив ШІ на людську природу.

Тема 3. **Етичні аспекти штучного інтелекту**

Упередженість та дискримінація

Як алгоритми ШІ можуть успадковувати та посилювати людські упередження. Приклади дискримінації в системах ШІ. Як боротися з упередженістю в ШІ.

Прозорість та пояснюваність

Чому важливо розуміти, як працюють алгоритми ШІ. Як зробити ШІ більш прозорим та пояснюваним. Виклики пояснювального ШІ.

Безпека та контроль

Потенційні ризики ШІ, такі як автономна зброя. Як забезпечити безпечний та відповідальний розвиток ШІ. Міжнародні норми та регулювання ШІ.

Психологічні та соціальні наслідки

Вплив ШІ на людську психологію та соціальні відносини. Етичні питання, пов'язані з штучною емпатією та маніпуляціями. Як зберегти людські цінності в епоху ШІ.

Тема 4. **Правові аспекти штучного інтелекту**

Інтелектуальна власність: авторське право, патенти, ноу-хау.

Відповідальність за шкоду, завдану ШІ-системами. Захист даних та приватності.

Міжнародні та національні нормативно-правові акти, що регулюють ШІ

Огляд основних міжнародних документів. Аналіз законодавства України про ШІ. Проблеми правового регулювання ШІ.

Майбутнє правового регулювання ШІ

Прогнози розвитку нормативно-правової бази. Шляхи вирішення проблем правового регулювання ШІ. Вплив ШІ на правову систему в цілому.

Тема 5. **ШІ в заходах кібербезпеки, в навчальному процесі, науковій діяльності**

Кібербезпека.

Виявлення та реагування на кіберзагрози. Захист даних. Прогнозування кібератак.

Навчання

Персоналізація навчання. Автоматизація завдань. Створення нових освітніх інструментів.

Наукова діяльність

Аналіз даних. Моделювання та прогнозування. Автоматизація

дослідницьких завдань.

Тема 6. **Використання ШІ в правозастосовній діяльності. Досудове, Судове розслідування**

Можливості використання ШІ на етапі досудового розслідування

Аналіз даних. Розпізнавання образів. Прогнозування поведінки. Автоматизація рутинних завдань.

Можливості використання ШІ на етапі судового розслідування

Аналіз доказів. Підготовка процесуальних документів. Оцінка ризиків. Прогнозування результатів судового розгляду.

Переваги та недоліки використання ШІ в правовій сфері

Прозорість та підзвітність алгоритмів ШІ. Захист персональних даних. Нейтральність та неупередженість ШІ-систем. Контроль над ШІ-системами.

Тема 7. **OSINT розслідування з використанням штучного інтелекту**

Джерела даних

Відкриті веб-сайти: соціальні мережі, форуми, блоги, новини. Глибока веб-павутина: закриті форуми, даркнет. Державні та комерційні бази даних

Інструменти та методи

Інструменти для пошуку інформації. Інструменти для аналізу інформації.

Методи OSINT розслідувань: геолокація, аналіз мови, OSINT-цикл

Штучний інтелект для OSINT

Аналіз великих даних: машинне навчання, NLP (Natural Language Processing). Виявлення аномалій: штучні нейронні мережі. Автоматизація завдань: чат-боти, віртуальні помічники. Обережність при зборі та аналізі даних. Повага до приватності. Відповідальність за поширення інформації

Приклади OSINT розслідувань з використанням ШІ

Розслідування військових злочинів. Виявлення терористичних груп. Розслідування кіберзлочинів

Тема 8. **Висновки**

Основні висновки курсу

Перспективи досліджень у галузі штучного інтелекту та кібербезпеки

5. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	ср		л	п	лаб	інд	ср
1	2	3	4	5	6	7	8	9	10	11	12	13

ТЕМА 1. Вступ до штучного інтелекту та кібербезпеки	14	2		4		8						
ТЕМА 2. Соціальні аспекти штучного інтелекту	16	2		4		10						
ТЕМА 3. Етичні аспекти штучного інтелекту	14	2		4		8						
ТЕМА 4. Правові аспекти штучного інтелекту	16	2		4		10						
ТЕМА 5. ШІ в заходах кібербезпеки, в навчальному процесі, науковій діяльності	14	2		4		8						
ТЕМА 6. Використання ШІ в правозастосовній діяльності. Досудове, Судове розслідування	14	2		4		8						
ТЕМА 7. OSINT розслідування з використанням штучного інтелекту	16	2		4		10						
ТЕМА 8. Висновки	16	2		4		10						
Усього годин	120	16		32		72						

6. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин

1	Вступ до штучного інтелекту та кібербезпеки	4
2	Соціальні аспекти штучного інтелекту	4
3	Етичні аспекти штучного інтелекту	4
4	Правові аспекти штучного інтелекту	4
5	ШІ в заходах кібербезпеки, в навчальному процесі, науковій діяльності	4
6	Використання ШІ в правозастосовній діяльності. Досудове, Судове розслідування	4
7	OSINT розслідування з використанням штучного інтелекту	4
8	Висновки	4

7. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1	Вступ до штучного інтелекту та кібербезпеки	8
2	Соціальні аспекти штучного інтелекту	10
3	Етичні аспекти штучного інтелекту	8
4	Правові аспекти штучного інтелекту	10
5	ШІ в заходах кібербезпеки, в навчальному процесі, науковій діяльності	8
6	Використання ШІ в правозастосовній діяльності. Досудове, Судове розслідування	8
7	OSINT розслідування з використанням штучного інтелекту	10
8	Висновки	10

8. МЕТОДИ НАВЧАННЯ

Серед методів навчання, зокрема, підлягають застосуванню такі: загальнонаукові і спеціальні методи пізнання правових явищ: логічний, проблемний, дослідницький, евристичний, ситуаційний, метод Сократа, групова дискусія, опрацювання аналітичних завдань, підготовка експертних висновків із проблемних питань, ділові/рольові ігри; кейс-стаді, дебати, виконання наукових робіт, практика з майбутньої професії, самостійна робота з літературою, Інтернет-ресурсами (самонавчання); методики з правової оцінки поведінки чи діяльності індивідів і соціальних груп, ідентифікація (розпізнавання) проблеми та її вирішення.

До освітніх технологій належать: інформаційно-комунікативні технології, аудіовізуальні технології, інтерактивні та мережеві технології, контекстного навчання, ситуативного моделювання, проектні технології, навчання як дослідження, модульно-блокового навчання.

9. МЕТОДИ КОНТРОЛЮ

Знання та навички студентів, отримані при засвоєнні навчальної дисципліни «Цифрова криміналістика», оцінюються за рейтинговою системою.

Форми поточного контролю включають: усне опитування, експрес-опитування, розв'язання практичних завдань/задач, підготовка і захист наукових робіт за ініціативою студента, peer review, захист кейсу, захист портфоліо, самооцінка студента за питаннями для самоконтролю, колоквіум.

Студент може отримати максимально 50 балів за усні відповіді або виконання контрольних робіт на практичних заняттях.

Неготовність до заняття або незадовільна відповідь (розв'язання) задачі також підлягають відповідній оцінці і студенту виставляється «0» балів. Отримані у такому разі «0» балів потребують відпрацювання та оцінка, одержана під час відпрацювання враховуються при визначенні середнього балу поточної успішності.

Формою підсумкового контролю знань та навичок по дисципліні для студентів є залік, який виставляється з урахуванням поточної успішності.

10. РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

Поточне тестування та самостійна робота				**Поточна успішність**	**Модуль**	**Сума**
Т1	Т2	Т3	Т4	Т. 1-4	Т. 1-5	100
				50	50	

Оцінювання знань студента здійснюється за 100 бальною шкалою

Шкала оцінювання: університету, національна та ECTS

Оцінка в балах	**Оцінка ECTS**	**Визначення**	**Екзаменаційна оцінка**
90-100	A	відмінно	відмінно
81-89	B	дуже добре	добре
71-80	C	добре	
61-70	D	задовільно	задовільно
51-60	E	достатньо	
до 51	FX	незадовільно з правом перездачі	незадовільно
до 51	F	незадовільно без права перездачі	

90-100 балів (відмінно) – виставляється студенту, який дав повну і правильну відповідь на всі питання, що базуються на знанні технічних аспектів питань, нормативно-правових актів, судової практики та спеціальної літератури. Прояви уміння застосування набуті знання до конкретних ситуацій дослідження

цифрової інформації та здібності аналізу джерел вивчення даного курсу.

81-89 балів (дуже добре) – виставляється студенту, який дав не цілком повну але правильну відповідь на всі питання, що базується на знанні предмету.

71-80 балів (добре) – виставляється студенту, який дав повну і правильну відповідь, але не на всі питання, або відповідь не базується на всіх складових джерелах вивчення. Тобто знав технічні аспекти питання, нормативно-правовий акт та судову практику але не знав інформації, що міститься у спеціальній літературі, чи інформації, яка міститься у інших джерелах. Однак у підсумку його відповідь повинна базуватись не менше ніж на двох базових джерелах.

61-70 балів (задовільно) – виставляється студенту, який не дав вичерпної детальної відповіді на питання контрольних завдань і яка базується тільки на одному із рекомендованих джерел вивчення матеріалу.

51-60 балів (достатньо) – виставляється студенту, який не дав вичерпної (достатньої) відповіді на питання контрольних завдань та не може назвати джерела інформації навчальної дисципліни.

0-50 балів (незадовільно) – виставляється студентові, який виявив значні прогалини в знаннях основного навчального матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань, незнайомий з основною літературою з дисципліни.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. AI and Fundamental Rights in Europe (2020) by the Fundamental Rights Agency (FRA).URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf.
2. AI Watch. Defining Artificial Intelligence 2.0.URL:https://publications.jrc.ec.europa.eu/repository/handle/JRC126426.
3. AI, Robotics and European Civil Liability Rules (2019) by the European Parliament Committee on Legal Affairs. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf.
4. Álvarez-Machancoses Ó, Fernández-Martínez JL. Using artificial intelligencemethods to speed up drug discovery. Expert Opin Drug Discov. (2019) 14:769–77. doi: 10.1080/17460441.2019.1621284
5. Asare J.G. The Dark Side Of ChatGPT. Forbes: Jersey City, NJ, USA, 2023. URL: https://www.forbes.com/sites/janicegassam/2023/01/28/the-dark-side-of-chatgpt/?sh=31f2e08a4799.
6. Barton C, Chettipally U, Zhou Y, Jiang Z, Lynn-Palevsky A, Le S, et al. Evaluation of a machine learning algorithm for up to 48-hour advance prediction of sepsis using six vital signs. Comput Biol Med. (2019) 109:79– 84. doi: 10.1016/j.compbiomed.2019.04.027
7. Basta C., Costa-jussà M. R., Casas, N. Evaluating the Underlying Gender Bias in

Contextualized Word Embeddings. Proceedings of the Workshop on Gender Bias in Natural Language Processing. 2019. 1. P. 33–39. URL: https://doi.org/10.18653/v1/W19-3805
8. Drukker L, Noble JA, Papageorghiou AT. Introduction to artificial intelligence in ultrasound imaging in Obstetrics and Gynecology. Ultrasound Obstetr Gynecol. (2020) 56:498–505. doi: 10.1002/uog.22122
9. Ethical Guidelines for Trustworthy AI (2018) by the High-Level Expert Group on AI.URL: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-uidelines.pdf.
10. Ethics Guidelines for Trustworthy AI (2019) by the European Commission's High-Level ExpertGroup on Artificial Intelligence.URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
11. Floridi L., Chiriatti, M. GPT-3: Its nature, scope, limits, and consequences. Minds and Machines. 2020. 30(4). P. 681-694. URL: https://doi.org/10.1007/s11023-020-09548-1
12. Getahun H. ChatGPT Could Be Used for Good, But Like Many Other AI Models, It's Rife with Racist and Discriminatory Bias; Insider. 2023. URL: https://www.insider.com/chatgpt-is-likemany-other-ai-models-rife-with-bias-023-1
13. Hay SI, George DB, Moyes CL, Brownstein JS. Big data opportunities for global infectious disease surveillance. PLoS Med. (2013) 10:e1001413. doi: 10.1371/journal.pmed.1001413
14. Henz P. Ethical and legal responsibility for artificial intelligence. Discov Artif Intell. (2021) 1:2. doi: 10.1007/s44163-021-00002-4
15. Hutchinson B., Prabhakaran V., Denton E., Webster K., Zhong Y., Denuyl S. Social Biases in NLP Models as Barriers for Persons with Disabilities. Proceedings of the Annual Meeting of the Association for Computational Linguistics. 2020. 58. P. 5491–5501. URL: https://doi.org/10.18653/v1/2020.acl-main.487
16. Jingshan Huang, Ming Tan. The role of ChatGPT in scientific communication: writing better scientific review articles. American Journal of Cancer Research. 2023. 13 (4). P. 1148-1154. URL: https://e-century.us/files/ajcr/13/4/ajcr0150104.pdf
17. Mannes A. Governance, risk, and Artificial Intelligence. AI Magazine. (2020) 41:61–9. doi: 10.1609/aimag.v41i1.5200
18. Miller DD, Brown EW. Artificial Intelligence in medical practice: the question to the answer? Am J Med. (2018) 131:129–33. doi: 10.1016/j.amjmed.2017.10.035
19. Morley J, Floridi L. An ethically mindful approach to AI for Health Care. SSRN Electron J. (2020) 395:254–5. doi: 10.2139/ssrn.3830536
20. Morley J, Machado CCV, Burr C, Cowls J, Joshi I, Taddeo M, et al. The ethics of AI in health care: a mapping review. Soc Sci Med. (2020) 260:113172. doi: 10.1016/j.socscimed.2020.113172
21. Nelson A, Herron D, Rees G, Nachev P. Predicting scheduled hospital attendance with Artificial Intelligence. npj Digit Med. (2019) 2:26. doi: 10.1038/s41746-019-0103-3
22. Nelson GS. Bias in artificial intelligence. North CarolinaMed J. (2019) 80:220–2. doi: 10.18043/ncm.80.4.220
23. Parikh RB, Teeple S, Navathe AS. Addressing bias in artificial intelligence in Health Care. JAMA. (2019) 322:2377. doi: 10.1001/jama.2019.18058
24. Perc M. The Matthew effect in empirical data. Journal of the Royal Society Interface. 2014.11(98).URL: https://doi.org/10.1098/rsif.2014.0378

25. Rong G, Mendez A, Bou Assi E, Zhao B, Sawan M. Artificial intelligence in healthcare: review and prediction case studies. Engineering. (2020) 6:291– 301. doi: 10.1016/j.eng.2019.08.015
26. Safdar NM, Banja JD, Meltzer CC. Ethical considerations in Artificial Intelligence. Eur J Radiol. (2020) 122:108768. doi:10.1016/j.ejrad.2019.108768
27. Shah M, Naik N, Somani BK, Hameed BMZ. Artificial Intelligence (AI) in urology-current use and future directions: an itrue study. Turk J Urol. (2020) 46(Suppl. 1):S27–S39. doi: 10.5152/tud.2020.20117
28. Smith H. Clinical AI: opacity, accountability, responsibility and liability. AI Soc. (2020) 36:535–45. doi: 10.1007/s00146-020-01019-6
29. Taddeo M, Floridi L. How AI can be a force for good. Science. (2018) 361:751–2. doi: 10.1126/science.aat5991
30. Taylor I. Who is responsible for killer robots? Autonomous Weapons, group agency, and the military-industrial complex. J Appl Philos. (2020) 38:320–34. doi: 10.1111/japp.12469
31. The AI Arms Race Is Changing Everything. TIME. URL: https://time.com/6255952/ai-impactchatgpt-microsoft-google/
32. The Ethics of Artificial Intelligence (2020) by the European Group on Ethics in
33. The Regulation of Artificial Intelligence in the European Union (2021) by the European Parliamentary Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.
34. White Paper on Artificial Intelligence - A European Approach to Excellence and Trust (2020) bythe European Commission. URL: https://commission.europa.eu/document/d2ec4039-c5be-423a81ef-b9e44e79825b_en.
35. Бєлов Д.М., Бєлова М.В. Система захисту прав і свобод людини і громадянина: доктринальні та нормативні основи. Науковий вісник Ужгородського національного університету. Серія «Право». 2022. Вип. 74. С. 85–90
36. Використання технологій штучного інтелекту для протидії злочинності. Матеріали науково-практичного онлайн-семінару.(Харків, 5 листопада 2020 р.), Харків «Право», 2020
37. Громовчук М.В., Бєлов Д.М. Гуманізм як філософсько-правова категорія в умовах формування нової парадигми в праві. Аналітично-порівняльне право. № 3/2022. С. 301–310.