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

Затверджено
на засіданні кафедри кримінального
процесу і криміналістики юридичного
факультету Львівського національного
університету імені Івана Франка
(протокол № від серпня 2024 року)

Завідувач кафедри _____ проф. Бобечко Н.Р.

Силабус з навчальної дисципліни

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

що викладається в межах ОПП Кібербезпека
першого (бакалаврського) рівня вищої освіти для здобувачів
зі спеціальності 125 – Кібербезпека

Львів – 2024

Назва дисципліни	Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Юридичний факультет Кафедра кримінального процесу і криміналістики
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека
Викладачі дисципліни	Мурадов Валентин Валентинович доцент кафедри кримінального процесу і криміналістики; Калужна Оксана Михайлівна, доцент кафедри кримінального процесу і криміналістики; Піх Юрій Тарасович, асистент кафедри кримінального процесу і криміналістики;
Контактна інформація викладачів	valentyn.muradov@lnu.edu.ua https://law.lnu.edu.ua/employee/muradov-valentyn-valentynovych oksana.kaluzhna@lnu.edu.ua https://law.lnu.edu.ua/employee/kaluzhna-oksana-myhajlivna yuriy.pikh@lnu.edu.ua https://law.lnu.edu.ua/employee/pikh-yuriy-tarasovych Місце знаходження: юридичний факультет, кафедра кримінального процесу і криміналістики, 79000, м. Львів, вул. Січових Стрільців, 14, ауд. Г-509, тел. (032) 239-47-40
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://law.lnu.edu.ua/course/sotsialni-etychni-ta-pravovi-aspekty-shtuchnoho-intelektu-ta-kiberbezpeky
Інформація про дисципліну	Дисципліна «Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки» є вибірковою дисципліною з спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 2 -му семестрі в обсязі 4-ти кредитів (за Європейськоюкредитно-трансферною системою ECTS).

Коротка анотація дисципліни	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 та цілі дисципліни	***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.

Література для вивчення дисципліни	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. AI Watch. Defining Artificial Intelligence 2.0. URL:https://publications.jrc.ec.europa.eu/repository/handle/JRC126426. 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. 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 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. 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 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 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 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. 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. 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 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 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 Henz P. Ethical and legal responsibility for artificial intelligence. Discov Artif Intell. (2021) 1:2. doi: 10.1007/s44163-021-00002-4 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 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 Mannes A. Governance, risk, and Artificial Intelligence. AI Magazine. (2020) 41:61–9. doi: 10.1609/aimag.v41i1.5200 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 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 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
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
Nelson GS. Bias in artificial intelligence. North CarolinaMed J. (2019) 80:220–2. doi: 10.18043/ncm.80.4.220
Parikh RB, Teeple S, Navathe AS. Addressing bias in artificial intelligence in Health Care. JAMA. (2019) 322:2377. doi: 10.1001/jama.2019.18058
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
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
Safdar NM, Banja JD, Meltzer CC. Ethical considerations in Artificial Intelligence. Eur J Radiol. (2020) 122:108768. doi:10.1016/j.ejrad.2019.108768
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
Smith H. Clinical AI: opacity, accountability, responsibility and liability. AI Soc. (2020) 36:535–45. doi: 10.1007/s00146-020-01019-6
Taddeo M, Floridi L. How AI can be a force for good. Science. (2018) 361:751–2. doi: 10.1126/science.aat5991
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
The AI Arms Race Is Changing Everything. TIME. URL: https://time.com/6255952/ai-impactchatgpt-microsoft-google/
The Ethics of Artificial Intelligence (2020) by the European Group on Ethics in
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.
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.
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
Використання технологій штучного інтелекту для протидії злочинності. Матеріали науково-практичного онлайн-семінару.(Харків, 5 листопада 2020 р.), Харків «Право», 2020
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.

	Ресурси: https://bard.google.com/ https://www.midjourney.com/home?callbackUrl=%2Fexplore https://chat.openai.com https://quickchat.ai https://copy.ai https://beatoven.ai https://synthesia.io https://soundraw.io https://ocoya.com https://unbounce.com https://inkforall.com https://musicgen.com/ https://rytr.me https://afforai.com/ Офіс Генерального прокурора України – https://www.gp.gov.ua/ СБУ – https://ssu.gov.ua/ НАБУ – https://nabu.gov.ua/ ДБР – https://dbr.gov.ua/ БЕБ – https://esbu.gov.ua/ Кіберполіція НП – https://cyberpolice.gov.ua/ Кіберцентр UA30 – https://cert.gov.ua/
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 72 год.
Очікувані результати навчання	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. **Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 4, КЗ 5, КФ 1, КФ 3, КФ 4, КФ 6, КФ 7, КФ 8, КФ 9, КФ 10; та програмних результатів навчання: ПРН 3, ПРН 4, ПРН 5, ПРН 9, ПРН 10, ПРН 12, ПРН 14, ПРН 32,ПРН 34, ПРН 50, ПРН 54.**

Ключові слова	Штучний інтелект, кібербезпека, етика ШІ, соціальні наслідки ШІ, правові аспекти ШІ, упередженість ШІ, прозорість ШІ, відповідальність ШІ, інтелектуальна власність ШІ, права людини в епоху ШІ, кіберзлочинність, алгоритми, автономія, біологічна безпека, глибоке навчання, дискримінація, зброя на основі ШІ, кіберстійкість, моральні дилеми, персоналізація, ризики ШІ, соціальна відповідальність, технологічна еволюція.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	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*
Підсумковий контроль, форма	Залік у кінці семестру

Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Серед методів навчання, зокрема, застосовуються: розповідь, пояснення, бесіда, лекція, демонстрація (презентація), спостереження, практичне заняття, індивідуальні завдання, дослідні проекти, модульний контроль Під час практичних занять забезпечується постановка питань на тлі змодельованих кейсів, пов'язаних з використанням спеціальних знань, їх обговорення з метою пошуку оптимальних шляхів вирішення практичної ситуації. На практичних заняттях викладач виконує роль модератора дискусії, визначає її напрями, забезпечує необхідну динаміку та загострює увагу на проблемних аспектах. Після завершення обговорення проблеми викладач підсумовує найважливіші моменти, аналізує сильні та слабкі сторони висловлених аргументів. Індивідуальні завдання студенти вирішують письмово, надсилаючи їх викладачеві на електронну пошту. Індивідуальні завдання мають пошуково-аналітичний характер – полягають у науковому обґрунтуванні неоднозначних ситуацій використанні ШІ та кібербезпеки. Вирішення індивідуальних запитань потребує не механістичного пошуку у літературі, компіляції з різних джерел, а завжди власного аналізу й вміння обґрунтувати свою позицію. Іноді на поставлені індивідуальні завдання немає строго єдино правильної відповіді, а відповідь буде варіативною залежно від додаткових деталей складових (змінних) кейсу (ситуації). Оцінюється ж глибина і всебічність мислення, аналізу, горизонт і масштаб бачення студентом проблеми.

Необхідне обладнання	Бакалаври використовують технічні засоби та програмне забезпечення під час підготовки до практичних занять з метою пошуку необхідної спеціальної літератури, нормативно-правових актів, а також під час виконання індивідуальних завдань
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • практичні заняття, індивідуальні завдання: 50% семестрової оцінки; • модуль: 50% семестрової оцінки. Максимальна кількість балів – 50 балів. Підсумкова максимальна кількість балів – 100 балів. **Оцінювання поточної успішності:** *Поточна успішність* (оцінюється за 50-бальною шкалою): – Відмінно (50) – Добре (40; 45) – Задовільно (26; 31) – Незадовільно (0) *Критерії оцінювання при виставленні заліку:* – **90-100 балів** (відмінно) – **81-89 балів** (добре) – **71-80 балів** (добре) – **61-70 балів** (достатньо) – **51-60 балів** (задовільно) – **0-51 балів** (незадовільно)

	50 балів – виставляється студенту, який дав повну і правильну відповідь на всі питання, що базуються на знанні нормативно-правових актів, судової, слідчої практики та спеціальної літератури; проявив уміння застосувати набуті знання до конкретних ситуацій та здібності аналізу джерел. **45 балів** – достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи у цьому нормативну та обов'язкову літературу. Але під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускає окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість завдань. Студент здатен виокремлювати суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно – наслідкові зв'язки, у яких можуть бути окремі несуттєві помилки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями. **40 балів** – за повну і правильну відповідь, але не на всі питання, або відповідь не базується на всіх складових джерелах вивчення. Тобто знав основне як для відповідної ситуації літературу, нормативно-правовий акт та слідчу, судову практику але не знав інформації, що міститься у спеціальній літературі, чи інформації, яка міститься у інших деталізованих джерелах. Однак у підсумку його відповідь повинна базуватись не менше ніж на двох базових джерелах. **31 бал** – виставляється студенту, який не дав вичерпної детальної відповіді на питання контрольних завдань і яка базується тільки на одному із рекомендованих джерел вивчення матеріалу.

	26 балів – в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних виступів та письмових вирішень, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи у цьому розрізі окремі суттєві неточності та помилки. Правильно вирішив половину письмових (в тому числі /тестових) завдань. Студент має труднощі з виокремлення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв'язків і формулювання висновків. **0 балів –** не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та вирішення домашніх завдань, недостатньо розкриває зміст теоретичних питань та практичних моделювань, допускаючи тут суттєві неточності. Безсистемне розмежування випадкових ознак вивченого; невміння робити найпростіші операції аналізу і синтезу; робити узагальнення, висновки. **Модуль:** Модуль здійснюється в тестовій формі з використанням програми Moodle – **https://e-learning.lnu.edu.ua/course/view.php?id=5187.** Модульне завдання для кожного студента включає 20 тестових запитань, з яких 10 першого рівня складності по 2 бали за правильну відповідь, і 10 – другого рівня по 3 (до 3-х) балів за правильну відповідь. У тестах першого рівня складності 4-5 варіантів відповідей, серед яких лише одна правильна. У тестах 2-го рівня складності є від 2 до 4 правильних відповіді серед понад 6 варіантів відповідей. Студенту потрібно обрали лише правильні відповіді. Вказування неправильної відповіді знімає бал, пропорційний до ціни (%) варіанта правильної відповіді. Студент має право перездати модуль за правилами перездач. На модуль виносяться лише питання, які розглядались на лекціях та лабораторних заняттях, відображені в презентації, текстах лекцій, наданих студентам викладачами. **Академічна доброчесність**: Очікується, що кожен студент повинен самостійно готуватися до практичних занять та вирішувати індивідуальні завдання, обдумувати та викладати власну аргументацію своєї правової позиції. Дві чи більше одинакові роботи студентів не перевіряються з виставлення кожному зі студентів 0 балів. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману; у разі незарахування роботи студент в узгоджені з викладачем строки повинен повторно виконати письмову роботу та подати її викладачу для оцінювання. **Відвідування занять** є добровільним для лекційної форми і обов'язковим для лабораторних. Викладач фіксує неявку студента на практичне заняття, що вважається академічною заборгованістю, яку студент повинен відпрацювати до дня виставлення заліку. Відпрацювання полягає у перевірці підготовки студентом тих самих завдань, які виносилися на практичне заняття, на якому студент був відсутній. **Література.** Уся література у вільному доступі в мережі Інтернет із наданням студентам лінків, на її розміщення. Лекції та презентації надаються студентам викладачем виключно в освітніх межах без права її

	передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані на практичних заняттях та за виконання індивідуальних завдань, бали одержані за модуль. Враховуються активність студента під час лабораторного заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття з метою не пов'язаною з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Критеріями оцінювання роботи студента на лабораторних заняттях є аргументованість наукової, правової позиції та її відповідність чинному законодавству; уміння лаконічно, переконливо та логічно висловити свою теоретико – правову позицію; здатність до аргументованого аналізу наукових і правових позицій у літературі, думок, висловлених іншими студентами; уміння підсумувати усі висловлені щодо певної проблеми аргументи і віднайти їхні сильні та слабкі сторони. **Жодні форми порушення академічної доброчесності не толеруються.**
Питання на модуль.	Що таке штучний інтелект (ШІ)? Які основні напрямки досліджень в ШІ? Як працюють алгоритми машинного навчання? Що таке нейронні мережі? Які етичні проблеми пов'язані з розвитком ШІ? Що таке кібербезпека? Які основні типи кібератак? Як захистити комп'ютер від вірусів та шкідливих програм? Як створити надійний пароль? Що таке шифрування даних? Назвіть кілька прикладів систем ШІ, які використовуються в реальному житті. Опишіть принцип роботи брандмауера. Що таке двофакторна аутентифікація? Які існують стандарти кібербезпеки? Як штучний інтелект може використовуватися для кібератак? Які основні соціальні проблеми, пов'язані з розвитком штучного інтелекту? Як штучний інтелект може вплинути на ринок праці? Які етичні питання виникають у зв'язку з використанням штучного інтелекту в медицині? Як штучний інтелект може вплинути на рівень злочинності? Які заходи можна вжити, щоб мінімізувати негативні соціальні наслідки штучного інтелекту? Як штучний інтелект може вплинути на демократію? Які можливості штучний інтелект відкриває для людей з обмеженими можливостями? Як штучний інтелект може вплинути на освіту? Які ризики пов'язані з автономною зброєю, що використовує штучний інтелект? Як штучний інтелект може вплинути на наше уявлення про себе? Які можливості штучний інтелект відкриває для творчості? Як штучний інтелект може вплинути на наше спілкування? Які етичні питання виникають у зв'язку з використанням штучного інтелекту в соціальних мережах? Як штучний інтелект може вплинути на нашу приватність? Які перспективи розвитку штучного інтелекту в найближчі роки? Які етичні питання виникають з розвитком штучного інтелекту? Як штучний інтелект може вплинути на людську автономію та приватність? Які ризики упередженості та дискримінації в системах штучного інтелекту? Як можна забезпечити справедливість та прозорість алгоритмів штучного інтелекту? Які етичні принципи розробки та використання штучного інтелекту? Як штучний інтелект може вплинути на ринок праці та зайнятість? Які етичні питання виникають при використанні штучного інтелекту в медицині? Як штучний інтелект може вплинути на безпеку та оборону? Які етичні питання виникають при використанні штучного інтелекту в автономних системах? Як штучний інтелект може вплинути на демократію та суспільство? Яка роль етики в регулюванні штучного інтелекту? Які міжнародні ініціативи з етики штучного інтелекту? Як штучний інтелект може вплинути на людську гідність та цінності? Яка відповідальність розробників, користувачів та регуляторів штучного інтелекту? Яке майбутнє етики штучного інтелекту? Що таке штучний інтелект з точки зору права? Які основні правові виклики, пов'язані з розвитком та використанням штучного інтелекту? Чи існують міжнародні правові акти, що регулюють штучний інтелект? Який правовий статус

	штучного інтелекту в Україні? Чи може штучний інтелект нести відповідальність за свої дії? Які питання інтелектуальної власності пов'язані з штучним інтелектом? Як штучний інтелект впливає на право на приватне життя? Які етичні принципи слід враховувати при розробці та використанні штучного інтелекту? Як штучний інтелект може використовуватися в правовій системі? Які ризики дискримінації пов'язані з використанням штучного інтелекту? Як штучний інтелект може вплинути на ринок праці? Які питання кібербезпеки пов'язані з штучним інтелектом? Які перспективи розвитку правового регулювання штучного інтелекту? Наведіть приклад успішного використання штучного інтелекту в правовій сфері. Які, на вашу думку, найважливіші правові питання, які потребують вирішення в контексті розвитку штучного інтелекту? Які основні напрямки використання ШІ в кібербезпеці? Як ШІ може допомогти у виявленні та реагуванні на кібератаки? Які етичні питання виникають при використанні ШІ в кібербезпеці? Які є приклади успішного використання ШІ для запобігання кіберзлочинам? Назвіть 3-5 інструментів на основі ШІ, що використовуються для захисту кібербезпеки. Які можливості використання ШІ в освіті? Як ШІ може допомогти персоналізувати навчання для кожного учня? Які є приклади успішного використання ШІ в освітніх проектах? Які виклики та ризики пов'язані з використанням ШІ в освіті? Як ШІ може допомогти викладачеві економити час та ресурси? Як ШІ використовується для пришвидшення наукових досліджень? Які нові можливості для наукових відкриттів дає ШІ? Які етичні питання виникають при використанні ШІ в науці? Назвіть 3-5 прикладів наукових проектів, де використовується ШІ. Як ШІ може допомогти у боротьбі з глобальними викликами, такими як зміна клімату? Що таке ШІ та які його основні можливості в контексті правозастосування? Які етичні питання виникають при застосуванні ШІ в правовій сфері? Як ШІ може використовуватися для прогнозування злочинів? Які інструменти на основі ШІ використовуються для аналізу даних у ході досудового розслідування? Як ШІ може допомогти в розпізнаванні та аналізі цифрових доказів? Які можливості ШІ для візуалізації даних у ході судового розслідування? Як ШІ може використовуватися для оцінки ризиків рецидиву злочинів? Які існують практики використання ШІ для визначення запобіжного заходу? Як ШІ може допомогти в автоматизації рутинних завдань у правозастосовній діяльності? Які перспективи розвитку та використання ШІ в правовій сфері? Які правові та нормативні акти регулюють використання ШІ в правозастосовній діяльності? Які міжнародні практики використання ШІ в правовій сфері? Які ризики та виклики використання ШІ в правовій сфері? Як можна забезпечити відповідальне та етичне використання ШІ в правозастосовній діяльності? Наведіть приклади успішного використання ШІ в розкритті та розслідуванні злочинів. Що таке OSINT? Які основні джерела інформації для OSINT-розслідувань? Як штучний інтелект може допомогти в OSINT-розслідуваннях? Які типи завдань OSINT можна автоматизувати за допомогою ШІ? Наведіть приклади інструментів ШІ, які використовуються для OSINT-розслідувань. Як штучний інтелект може допомогти в аналізі даних OSINT? Які етичні міркування слід враховувати при використанні ШІ для OSINT-розслідувань? Як штучний інтелект може допомогти в розкритті кіберзлочинів? Як штучний інтелект може допомогти в розслідуваннях тероризму? Як штучний інтелект може допомогти в розслідуваннях організованої злочинності? Які виклики та обмеження використання ШІ для OSINT-розслідувань? Як штучний інтелект може допомогти в розслідуваннях зникнення людей? Як штучний інтелект може допомогти в розслідуваннях військових злочинів? Як штучний інтелект може допомогти в розслідуваннях порушень прав людини? Як штучний інтелект може допомогти в розслідуваннях корупції?

Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.