Силабус дисципліни "Гібридні загрози та штучний інтелект"

№	Назва поля	Контент, коментарі
1.	Рівень вищої освіти	Другий (магістерський)
2.	Спеціальність	F3 Комп'ютерні науки
3.	Тип і назва освітньої програми	Освітньо-професійна програма Системи штучного інтелекту
4.	Статус дисципліни	Основна
5.	Мова викладання	Українська
6.	Кількість ЄКТС кредитів	5
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 24 годин, практичні заняття – 8 годин, лабораторні роботи – 20 годин, консультації – 8 годин, самостійна робота – 90 годин
8.	Форма підсумкового контролю	Іспит
9.	Графік (терміни) вивчення дисципліни	1 рік (курс), 1 семестр
10.	Цілі навчання за дисципліною	Надати знання та навички, необхідні для попередження гібридних впливів, виявлення гібридних кампаній, планування і реалізацію ефективних відповідей на них в сфері штучного інтелекту
11.	Результати навчання	• Ідентифікувати поняття, алгоритми та структури даних необхідні для опису предметної області розробки або дослідження, пов'язаної з гібридними загрозами; забезпечити декомпозицію поставленої задачі з метою застосування відомих методів і технологій для її вирішення. • Обирати належні засоби для розробки або дослідження (наприклад, середовище розробки, мова програмування, програмне забезпечення та програмні пакети), що дозволяють знайти правильне і ефективне рішення в галузі безпеки в умовах гібридних впливів. • Володіти принципами, техніками та засобами розробки або дослідження, що використовуються у предметній області розробки або дослідження, пов'язаній з гібридними загрозами; створювати прототипи програмного забезпечення, щоб переконатися, що воно відповідає вимогам до розробки; виконувати його тестування і статичний аналіз, щоб переконатися у відповідності завданню розробки або дослідження • Демонструвати здатність участі у колективній роботі, використання інструментів колективної розробки чи дослідження. • Аналізувати сучасні світові тенденції розвитку комп'ютерних наук, штучного інтелекту та технологій забезпечення безпеки від гібридних загроз.
12.	Анотація (зміст) дисципліни	Модуль 1. Вступ до нового ландшафту глобальної безпеки

		Тема 1. Орієнтація в сучасному ландшафті штучного інтелекту. Великі мовні моделі (LLMs), трансформери, їхні сильні сторони та вразливості. Тема 2. Вплив штучного інтелекту на гібридну війну: кіберпідсилені гібридні загрози (деструктивне використання ШІ, розширення ролі кіберпростору під час криз, залежність суспільства від технологій). Модуль 2. Безпека штучного інтелекту Тема 1. Вступ до проєктування та розробки безпечного програмного забезпечення. Концепції безпеки: вразливості, загрози та атаки. Основи безпеки програмного забезпечення. Тема 2. Безпека інтелектуального програмного забезпечення. Стійкість і надійність тренування та функціонування моделей ШІ. Тема 3. Атаки на машинне навчання: види, визначення, наслідки, протидії. Глибоке навчання та безпека; атаки на комп'ютерний зір. Тема 4. Використання штучного інтелекту для кібербезпеки: атрибуція атак; виявлення зловмисної активності. Теорія ігор для забезпечення безпеки. Модуль 4. Прийняття рішень та розв'язання проблем у ворожому середовищі Тема 1. Теорія ігор для прийняття рішень у ворожих умовах. Тема 2. Аналіз розвідувальної інформації; оцінка конкуруючих гіпотез. Модуль 5. Управління інформацією в умовах гібридної війни Тема 1. Пошук інформації; дезінформація; криптографія; перевірка інформації. Тема 2. Боротьба з дезінформацією за допомогою штучного інтелекту.
13.	Система оцінювання	Нарахування балів за курс: • воркшопи (3 практичні заняття) – 30 балів, • майстер-клас (1 практичне заняття з фактчекінгу) – 10 балів, • адверсаріальні ігри (1 практичне заняття: тренування генеративних змагальних мереж) – 20 балів, • іспит – 40 балів. Максимум – 100 балів.
14.	Якість освітнього процесу	Дотримання принципів академічної доброчесності здійснюється відповідно до Положення ХНУРЕ про протидію академічному плагіату та принципам академічної доброчесності, викладеним в Положенні про організацію освітнього процесу в ХНУРЕ, п.5.8

		Інструментом контрольних заходів є рейтингове оцінювання студентів. Кожний бал надається за конкретне досягнення, перелік яких оприлюднюється на початку курсу. Протягом семестру студенти "набирають" певну кількість балів за результати своєї роботи. Всі практичні та лабораторні роботи мають груповий характер та виконуються на занятті. Присутність студента на занятті є необхідною умовою для отримання 100% оцінки. Відсутність, але вчасне виконання завдання є необхідною умовою для отримання 80% оцінки; відсутність та виконання завдання поза дедлайном дозволить отримати не більш ніж 70% оцінки. По завершенню курса проводиться анонімне опитування студентів для отримання зворотнього зв'язку щодо корисності запропонованого матеріалу та складності виконання роботи.
15.	Сторінка курсу на платформі Moodle	*https://dl.nure.ua/*
16.	Література	Електорнний ресурс: Європейський центр з протидії гібридним загрозам Hybrid CoE https://www.hybridcoe.fi/ Глосарій гібридних загроз https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Kurakin, A., Goodfellow, I., & Bengio, S. (2016). Adversarial machine learning at scale. arXiv preprint arXiv:1611.01236. Ivan, C., Chiru, I., & Arcos, R. (2023). Hybrid Security Threats and the Information Domain: Concepts and Definitions. In *Routledge Handbook of Disinformation and National Security* (pp. 9-19). Routledge. Thiele, R. (2020). Hybrid CoE Working Paper 6. Artificial Intelligence – A key enabler of hybrid warfare. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf Jerbi, S., Gyurik, C., Marshall, S. C., Molteni, R., & Dunjko, V. (2024). Shadows of quantum machine learning. *Nature Communications*, *15*(1), 5676.

		Stenzel, G., Zorn, M., Altmann, P., Mansky, M. B., Kölle, M., & Gabor, T. (2024, July). Self-Replicating Prompts for Large Language Models: Towards Artificial Culture. In *ALIFE 2024: Proceedings of the 2024 Artificial Life Conference*. MIT Press.
17.	Матеріально-технічне, лабораторне, програмне забезпечення дисципліни	Спеціалізована навчальна лабораторія ШІ є складовою міжфакультетського хабу ХНУРЕ з протидії гібридним загрозам, а також – учасником міжгалузевого середовища з протидії гібридним загрозам WARN. В 2021 році лабораторія ШІ отримала потужне комп'ютерне обладнання на загальну суму більш ніж 420 тис.грн, профінансоване грантом проєкту Еразмус+ "Академічна протидія гібридним загрозам – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
18.	Кафедра	Кафедра штучного інтелекту (ШІ), ауд. 245, 255 - 258 Тел. +38(057)7021337, http://ai.nure.ua d_ai@nure.ua
19.	Викладач(і) – розробник(и) силабусу	Доцент Марія Головянко, к.т.н, доцент, mariia.golovianko@nure.ua