Силабус дисципліни **"Гібридні загрози та комплексна безпека"**

№	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	Обов'язковий компонент
5.	Мова викладання	Українська
6.	Кількість ЄКТС кредитів	*5*
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 30 годин, практичні заняття – 20 годин, консультації – 10 годин, самостійна робота – 90 годин
8.	Форма підсумкового контролю	Залік
9.	Графік (терміни) вивчення дисципліни	1 рік (курс), 1 семестр
10.	Цілі навчання за дисципліною	Надати знання та навички, необхідні для розуміння, аналізу та реагування на гібридні загрози в професійній діяльності та громадському житті
11.	Результати навчання	• Демонструвати здатність участі у колективній роботі, використання інструментів колективної розробки чи дослідження. • Вміти спілкуватися з людьми, які не є професіоналами у галузі комп'ютерних наук, з метою виявлення їх потреб щодо комп'ютерізації поцесів, до яких вони залучені. • Враховувати соціально-економічні аспекти проєкту в контексті завдання розробки або дослідження, зокрема несуперечливість технічного прогресу і етичних стандартів • Аналізувати сучасні світові тенденції розвитку комп'ютерних наук та уявляти перспективи розвитку інформаційних технологій. • Демонструвати розуміння комплексної природи, складності, логіки і закономірностей гібридних загроз. • Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.
12.	Анотація (зміст) дисципліни	Модуль 1. Вступ до гібридних загроз Тема 1. Новий ландшафт безпеки, війна і мир Тема 2. Гібридні загрози - історія, визначення, основні характеристики: асиметрія, синхронізований пакет атак, креативність і неоднозначність, дії нижче порогу Модуль 2. Концептуальна модель гібридних загроз Тема 1. Ландшафт гібридних загроз: передумови, елементи та структура моделі Тема 2. Державні та недержавні актори, їх використання в гібридному впливі

		Модуль 3. Домени зловмисних дій Тема 1. Спектр PMESII: інформація, кіберпростір, космос, економіка, військові/оборонні, культура, соціальні/суспільні, державне управління, правові, розвідувальні, дипломатія, політика, інфраструктурні домени Тема 2. Кіберпростір і безпека штучного інтелекту Модуль 4. Інструменти та фази гібридної активності Тема 1: Система інструментів гібридного впливу; операції проти інфраструктури; кібершпигунство та кібероперації, електронні операції, економічні, військові/парамілітарні, соціокультурні, інструменти в державному управлінні, правові, розвідувально-дипломатичні, інформаційно-аналітичні, медійні інструменти Тема 2. Критичні функції та вразливості, прийняття рішень під загрозою, операції проти критичної інфраструктури. Динаміка гібридних загроз: роль різних видів діяльності в ландшафті гібридних загроз; фази гібридних загроз, гібридна активність Модуль 5. Протидія гібридним загрозам Тема 1. Концепція комплексної безпеки (на прикладі фінської моделі). Модель CORE. Побудова стійкості (включаючи приклади з тренінгів в ЄС, наприклад, скандал з відмиванням грошей у Danske Bank), адаптивний цикл Голлінга, панархія Тема 2. Побудова стратегії протидії гібридним загрозам: виявлення (моніторинг проти виявлення), стримування шляхом заперечення, стримування шляхом покарання, реагування
13.	Система оцінювання	Накопичування балів з навчальної дисципліни: • воркшопи (1 практичну заняття) – 20 балів, • майстер-класи (2 практичні заняття) – 40 балів, • командні ігри (1 практичні заняття з ділема-гри) – 20 балів, • брейнштормінг (1 практичне заняття) – 20 балів. Максимальна кількість балів – 100 (60 та більше – зараховано, 59 та менше – не зараховано)
14.	Якість освітнього процесу	Процедури дотримання принципів академічної доброчесності регламентуються Положенням ХНУРЕ про протидію академічному плагіату та принципами академічної доброчесності, викладеними 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" бали за результати своєї роботи. Всі практичні роботи мають індивідуальний характер та виконуються на занятті. Присутність студента на занятті є необхідною умовою для отримання 100% оцінки. Вчасне виконання завдання (при відсутності на занятті) є необхідною умовою для отримання 80% оцінки; виконання завдання поза дедлайном (при відсутності на занятті) 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	Електронний 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 MCDC (2017), Understanding Hybrid Warfare. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare MCDC (2019), Countering Hybrid Warfare, 2019. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem,

		Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.
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