

	СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Гібридні загрози та штучний інтелект» Рівень вищої освіти: <u>Другий (магістерський)</u> Спеціальність: <u>ЕЗ Комп'ютерні науки</u> Рік навчання: <u>1-й, семестр 3-й</u> Кількість кредитів ECTS: <u>4 кредитів</u> Назва кафедри: <u>Комп'ютерних наук та цифрової економіки</u> Мова викладання: <u>українська</u>
Лектор курсу	к.т.н, старший викладач Титарчук Євгеній Олександрович
Контактна інформація лектора (e-mail)	<u>etitarchuk@gmail.com</u>

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Гібридні загрози та штучний інтелект» є вибірковою компонентою ОПП.

Загальний обсяг дисципліни 120 год.: лекції – 16 год.; практичні заняття – 0 год., самостійна робота – 90 год.

Формат проведення: лекції, практичні заняття, консультації.

Підсумковий контроль – екзамен.

Призначення навчальної дисципліни

Дисципліна «Гібридні загрози та штучний інтелект» спрямована надати здобувачам здатність аналізувати гібридні загрози, виявляти кіберризики та інформаційно-психологічні впливи, застосовувати штучний інтелект для захисту даних і критичної інфраструктури, оцінювати безпеку моделей, проєктувати кіберстійкі системи та дотримуватися правових і етичних вимог.

Мета вивчення навчальної дисципліни

Метою навчальної дисципліни «Гібридні загрози та штучний інтелект» є формування у здобувачів освіти системи теоретичних знань і практичних навичок, необхідних для виявлення, оцінювання та протидії гібридним загрозам у цифровому середовищі із застосуванням технологій штучного інтелекту, а саме: ознайомлення студентів із сутністю та еволюцією гібридних загроз, кіберзагрозами, інформаційно-психологічними операціями, соціальною інженерією, безпекою критичної інформаційної інфраструктури, методами захисту даних і моделей штучного інтелекту, а також розвиток здатності до

моделювання кіберризиків і проектування кіберстійких систем з урахуванням правових та етичних засад.

Завдання вивчення дисципліни

Завданням дисципліни є ознайомлення з поняттями, еволюцією та основними проявами гібридних загроз; формування знань про кіберзагрози в цифровому середовищі, критичну інформаційну інфраструктуру, інформаційно-психологічні операції, соціальну інженерію та роль людського чинника; вивчення основ і технологій штучного інтелекту, його застосування для виявлення кіберзагроз та проведення інформаційних операцій, а також аналіз атак на системи штучного інтелекту й засобів захисту даних і моделей. Курс спрямований на набуття студентами теоретичних і практичних умінь щодо автономних кібероперацій, використання інтелектуальних програмних агентів, протидії гібридним загрозам, моделювання та оцінювання кіберризиків, дотримання правових і етичних засад застосування штучного інтелекту. Особлива увага приділяється формуванню навичок проектування кіберстійких систем із використанням штучного інтелекту, розвитку аналітичного мислення, здатності виявляти, оцінювати й нейтралізувати загрози, а також ухвалювати обґрунтовані рішення в умовах невизначеності.

ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ, ЯКИХ НАБУВАЄ ЗДОБУВАЧ ПРИ ВИВЧЕНІ ДИСЦИПЛІНИ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

У результаті вивчення навчальної дисципліни здобувач повинен сформувати такі програмні компетентності:

інтегральну компетентність (ІК):

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері комп'ютерних наук.

загальні компетентності (ЗК):

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність вчитися й оволодівати сучасними знаннями.

ЗК6. Здатність бути критичним і самокритичним.

ЗК7. Здатність генерувати нові ідеї (креативність).

спеціальні (фахові, предметні) компетентності (СК):

СК2. Здатність формалізувати предметну область певного проєкту у вигляді відповідної інформаційної моделі.

СК3. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області.

СК4. Здатність збирати і аналізувати дані (включно з великими), для забезпечення якості прийняття проєктних рішень.

СК5. Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

СК6. Здатність застосовувати існуючі і розробляти нові алгоритми розв'язування задач у галузі комп'ютерних наук.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

РН1. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань.

РН2. Мати спеціалізовані уміння/навички розв'язання проблем комп'ютерних наук, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур.

РН6. Розробляти концептуальну модель інформаційної або комп'ютерної системи.

РН10. Проектувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

РН13. Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

РН18. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

РН19. Аналізувати сучасний стан і світові тенденції розвитку комп'ютерних наук та інформаційних технологій.

Вивчення даної дисципліни формує у здобувачів освіти соціальні навички (soft skills): комунікативність (реалізується через: метод роботи в парах та групах, робота з інформаційними джерелами), робота в команді (реалізується через: метод проєктів), лідерські навички (реалізується через: робота в групах, метод проєктів, метод самопрезентації).

ПЛАН ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Назви теми	Форми організації навчання та кількість годин		Самостійна робота, кількість годин
		лекційні заняття	практичні заняття	
3-й семестр				
1	Тема 1. Поняття та еволюція гібридних загроз	2	0	12
2	Тема 2. Соціальна інженерія та людський фактор	2	0	12
3	Тема 3. ІІІ для виявлення кіберзагроз	2	0	12
4	Тема 4. Атаки на системи штучного інтелекту	2	0	12
5	Тема 5. Безпека даних і моделей ІІІ	2	0	12
6	Тема 6. Автономні кібероперації та агенти ІІІ	2	0	10
7	Тема 7. Методи протидії гібридним загрозам	2	0	10
8	Тема 8. Проектування кіберстійких систем із використанням ІІІ	2	0	10
Разом		16	0	90

Самостійна робота здобувача вищої освіти

Самостійна робота здобувача організовується шляхом видачі індивідуального переліку питань і практичних завдань з кожної теми, які не виносяться на аудиторне опрацювання та виконання індивідуального творчого завдання.

Самостійна робота здобувача є одним із способів активного, цілеспрямованого набуття нових для нього знань та умінь. Вона є основою його підготовки як фахівця, забезпечує набуття ним прийомів пізнавальної діяльності, інтерес до творчої роботи, здатність вирішувати наукові та практичні завдання.

Виконання здобувачем самостійної роботи передбачає, за необхідності, отримання консультацій або допомоги відповідного фахівця. Навчальний матеріал навчальної дисципліни, передбачений робочою програмою для засвоєння здобувачем у процесі самостійної роботи, виносяться на поточний і підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався під час аудиторних занять. Організація самостійної роботи здобувачів передбачає: планування обсягу, змісту, завдань, форм і методів контролю самостійної роботи, розробку навчально-методичного забезпечення; виконання здобувачем запланованої самостійної роботи; контроль та оцінювання результатів, їх систематизацію, оцінювання ефективності виконання здобувачем самостійної роботи.

Індивідуальні завдання здобувач виконує самостійно під керівництвом

викладача згідно з індивідуальним навчальним планом.

У випадку реалізації індивідуальної освітньої траєкторії здобувача заняття можуть проводитись за індивідуальним графіком.

Види самостійної роботи

№ п/п	Вид самостійної роботи	Години	Термін виконання	Форма та метод контролю
1	Підготовка самостійних питань з тематики дисципліни (опрацювання теоретичних основ прослуханого лекційного матеріалу)	465	щотижнево / під час заліково-екзаменаційно ї сесії	Усне та письмове опитування, тестування, оцінювання конспекту
2	Підготовка до лекційних та практичних занять (робота з інформаційними джерелами: опрацювання першоджерел)	10	щотижнево	Усне опитування, оцінювання конспекту
3	Індивідуальні творчі практичні завдання (вирішення і письмове оформлення завдань, інших робіт графічного характеру; презентації за заданою проблемною тематикою)	10	1 раз на 2 тижні / під час заліково-екзаменаційно ї сесії	Спостереження за виконанням, обговорення, виступ з презентацією
4	Підготовка до контрольних робіт та тестування, виконання завдань різних видів контролю під час практичних занять (самостійне опрацювання тестів відповідно до теми практичного заняття; самостійне розв'язання практичних задач, ситуаційних вправ)	10	щотижнево / під час заліково-екзаменаційно ї сесії	Тестування у системі Moodle
Разом		90		

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні

1. The Landscape of Hybrid Threats: A Conceptual Model (Public Version) / P. Cullen et al. ; ed. by G. Giannopoulos, H. Smith, M. Theocharidou. Luxembourg : Publications Office of the European Union, 2021. DOI: 10.2760/44985.
2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed., Global ed. Harlow : Pearson, 2021. 1168 p.
3. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD : National Institute of Standards and Technology, 2023. NIST AI 100-1. DOI: 10.6028/NIST.AI.100-1.
4. Vassilev A., Oprea A., Fordyce A., Anderson H. et al. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations.

Gaithersburg, MD : National Institute of Standards and Technology, 2025. NIST AI 100-2 E2025. DOI: 10.6028/NIST.AI.100-2e2025.

5. ENISA Threat Landscape 2024. Athens : European Union Agency for Cybersecurity (ENISA), 2024.

6. OWASP Top 10 for LLM Applications 2025. Wilmington, DE : OWASP Foundation, 2024. URL: <https://genai.owasp.org/llm-top-10/> (дата звернення: 09.10.2026).

Додаткові

1. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с. DOI: 10.53679/NISS-book.2022.01.

2. Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations / J. A. Goldstein et al. arXiv. 2023. arXiv:2301.04246. DOI: 10.48550/arXiv.2301.04246.

3. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile / C. Autio et al. Gaithersburg, MD : National Institute of Standards and Technology, 2024. NIST AI 600-1. DOI: 10.6028/NIST.AI.600-1.

4. Mirsky Y., Lee W. The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys. 2021. Vol. 54, no. 1. Art. 7. DOI: 10.1145/3425780.

5. Mirsky Y., Demontis A., Kotak J. et al. The Threat of Offensive AI to Organizations. Computers & Security. 2023. Vol. 124. Art. 103006.

6. Scharre P. Four Battlegrounds: Power in the Age of Artificial Intelligence. New York : W. W. Norton & Company, 2023.

7. International AI Safety Report / Y. Bengio et al. London : Department for Science, Innovation and Technology, 2025. arXiv:2501.17805.

8. 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). Official Journal of the European Union. 2024. L series, 12.7.2024.

9. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 09.10.2026).

10. Горбатенко В. Ескалація гібридної війни: новітні виклики і засоби протидії. Політологічний вісник. 2025. Вип. 99. С. 263–275. DOI: 10.17721/2415-881x.2025.99.263-275.

Інформаційні ресурси

1. European Centre of Excellence for Countering Hybrid Threats (Hybrid

CoE) : офіційний вебсайт. URL: <https://www.hybridcoe.fi/> (дата звернення: 02.10.2026).

2. Summary of NATO's Revised Artificial Intelligence (AI) Strategy / NATO. 10 July 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy> (дата звернення: 02.10.2026).

3. EUvsDisinfo : платформа моніторингу та аналізу дезінформації. URL: <https://euvsdisinfo.eu/> (дата звернення: 02.10.2026).

4. European Union Agency for Cybersecurity (ENISA) : офіційний вебсайт. URL: <https://www.enisa.europa.eu/> (дата звернення: 02.10.2026).

5. Центр протидії дезінформації : офіційний вебсайт. URL: <https://cpd.gov.ua/> (дата звернення: 02.10.2026).

СИСТЕМА ОЦІНЮВАННЯ ТА ВИМОГИ ДО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

У кінці семестру, здобувач вищої освіти може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру, до 10% за показники наукової, інноваційної, навчальної, виховної роботи та студентської активності і до 30% підсумкової оцінки – за результатами підсумкового контролю.

Розподіл балів за видами навчальної діяльності

№ п.п.	Вид навчальної діяльності	Бали
Атестація 1.		
1	Участь у дискусіях на лекційних заняттях	4
2	Участь у роботі на практичних заняттях	0
3	Виконання контрольних робіт, тестування	5
4	Підготовка самостійних питань з тематики дисципліни	21
	Всього за атестацію 1	30
Атестація 2.		
1	Участь у дискусіях на лекційних заняттях	4
2	Участь у роботі на практичних заняттях	0
3	Виконання контрольних робіт, тестування	5
4	Підготовка самостійних питань з тематики дисципліни	21
	Всього за атестацію 2	30
	Показники наукової, інноваційної, навчальної, виховної роботи та студентської активності	10
	Підсумкове тестування	30
Разом		100

У кінці семестру, здобувач вищої освіти може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру, до

10% за показники наукової, інноваційної, навчальної, виховної роботи та студентської активності і до 30% підсумкової оцінки – за результатами підсумкового контролю.

Якщо здобувач упродовж семестру за підсумками контрольних заходів набрав (отримав) менше половини максимальної оцінки з навчальної дисципліни (менше 35 балів), то він не допускається до екзамену. Крім того, обов'язковим при мінімальній кількості балів за підсумками контрольних заходів є виконання індивідуальної творчої роботи (презентації).

Під час виконання навчальних завдань, а також завдань поточних та підсумкових контрольних заходів не допустимо порушення академічної доброчесності. Презентації та виступи мають бути авторськими та оригінальними, інформація про результати власної навчальної (наукової, творчої) діяльності – достовірною; у разі використання ідей, розробок, тверджень, відомостей мають бути посилання на джерела інформації з дотриманням норм законодавства про авторське право і суміжні права.

Програма навчальної дисципліни передбачає врахування результатів неформальної та інформальної освіти при наявності підтверджуючих документів як окремі кредити вивчення навчальних дисциплін.

Переведення балів внутрішньої 100-бальної шкали в національну здійснюється у відповідності до шкали.

Відповідність шкал оцінок якості засвоєння навчального матеріалу

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
75-81	C		
66-74	D	задовільно	
60-65	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни