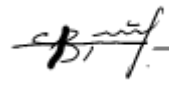


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Львівський національний університет імені Івана Франка**  
**Факультет прикладної математики та інформатики**  
**Кафедра кібербезпеки**

**Затверджено**

на засіданні кафедри кібербезпеки  
факультету прикладної математики та  
інформатики  
Львівського національного університету  
імені Івана Франка  
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри



П.С.Венгерський

**Силабус з навчальної дисципліни**  
**“ Застосування систем штучного інтелекту в кібербезпеці ”,**  
**що викладається в межах ОПП Кібербезпека**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності 125 – кібербезпека та захист інформації**

**Львів 2023 р.**

<b>Назва дисципліни</b>	<b>Системи штучного інтелекту</b>
<b>Адреса викладання дисципліни</b>	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики кафедра кібербезпеки
<b>Галузь знань, шифр та назва спеціальності</b>	12 – інформаційні технології 125 – кібербезпека та захист інформації
<b>Викладачі дисципліни</b>	Пелешко Дмитро Дмитрович, професор кафедри кібербезпеки Колос Надія Мирославівна, доцент кафедри дискретного аналізу та інтелектуальних систем.
<b>Контактна інформація викладачів</b>	dmytro.peleshko@lnu.edu.ua <a href="mailto:nadiya.kolos@lnu.edu.ua">nadiya.kolos@lnu.edu.ua</a> Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська, 1
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/academics/bachelor">https://ami.lnu.edu.ua/academics/bachelor</a>
<b>Інформація про дисципліну</b>	Дисципліна “Застосування систем штучного інтелекту в кібербезпеці” є нормативною дисципліною для спеціальності 125 – Кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 6-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Коротка анотація дисципліни</b>	Штучний інтелект - один з найперспективніших напрямків комп'ютерних наук, який вивчає методи розв'язання задач, для яких не існує способів вирішення. Системи штучного інтелекту можуть оперувати даними та самонавчатися. Сфери застосування таких систем є необмеженими - від створення роботів, які самостійно приймають рішення, до машин з автопілотом чи онлайн-перекладачів в реальному часі.
<b>Мета та цілі дисципліни</b>	Метою даного курсу є ознайомити студентів з основними підходами до вирішення інтелектуальних задач; сформулювати освоєння основних принципів побудови та функціонування інтелектуальних систем; виробити навички та вміння по вибору методів та алгоритмів для вирішення типових інтелектуальних задач. Цей курс містить фундаментальні положення систем штучного інтелекту, а також головні моделі й універсальні процедури, застосовні до широкого кола задач, які важко піддаються розв'язуванню традиційними методами.
<b>Література для вивчення дисципліни</b>	<b>Основна література:</b> 1. Булгакова О.С., Зосімов В.В., Поздеев В.О. Методи та системи штучного інтелекту: теорія та практика, - Вид-во Гельветика, 2020. – 356 ст. 2. Artificial Intelligence. A Modern Approach. (4th Edition). Stuart J. Russell and Peter Norvig. – 4d ed., - Pearson Education, 2020/ - 1136 p. 3. I, Human: AI, Automation, and the Quest to Reclaim What Makes Us Unique Kindle Edition. Tomas Chamorro-Premuzic. - Harvard Business Review Press, 2023. – 220 p.

	<p>4. Троцько В.В. Методи штучного інтелекту: навчально-методичний і практичний посібник, К.: Університет "КРОК", 2020. – 86 с.</p> <p>5. Шаповал Н.В. Методи та системи штучного інтелекту. Комп'ютерний практикум [Електронний ресурс], - КПІ ім. Ігоря Сікорського, 2022. – 44 ст. - <a href="https://ela.kpi.ua/bitstream/123456789/57162/1/Shapoval_SMSHl.pdf">https://ela.kpi.ua/bitstream/123456789/57162/1/Shapoval_SMSHl.pdf</a></p> <p><b>Додаткова література:</b></p> <ol style="list-style-type: none"> <li>1. Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина, Системи штучного інтелекту, Львів, 2010.</li> <li>2. Савченко А.С., Синельников О.О. Методи та системи штучного інтелекту – К. : НАУ, 2017. – 190 с.</li> <li>3. Luger, George F. Artificial intelligence : structures and strategies for complex problem solving / George F. Luger.-- 6th ed., - University of New Mexico, 2009. – 779 p.</li> <li>4. Haykin S. Neural networks and learning machines / Simon Haykin.—3rd ed. Pearson, 2018. – 938 с.</li> </ol>
<b>Обсяг курсу</b>	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 години лабораторних занять. Самостійної роботи: 56 годин.
<b>Очікувані результати навчання</b>	<p>Після завершення цього курсу студент буде:</p> <ul style="list-style-type: none"> <li>• <b>знати:</b> <ul style="list-style-type: none"> <li>– основні методи використання технологій штучного інтелекту для задач кібербезпеки</li> <li>– формулювання основних понять і означень штучного інтелекту;</li> <li>– способи подання задач і методи пошуку розв'язків;</li> <li>– базові концепції та загальну характеристику інтелектуальних систем;</li> <li>– основні класичні підходи до вирішення типових інтелектуальних задач;</li> <li>– основи моделювання та представлення знань (фреймові, семантичні логічні моделі);</li> <li>– основи формалізації експертних знань та основні принципи створення та функціонування експертних систем.</li> </ul> </li> <li>• <b>вміти:</b> <ul style="list-style-type: none"> <li>– використовувати технології штучного інтелекту для задач кібербезпеки</li> <li>– формалізувати знання за допомогою різних способів представлення знань;</li> <li>– розробляти модульну інтелектуальну систему на модельному та концептуальному рівні;</li> <li>– проектувати інтелектуальні системи, експертні системи, бази знань;</li> <li>– використовувати інтелектуальні системи для вирішення прикладних завдань у кібербезпеці.</li> </ul> </li> </ul> <p><b>Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 2, КФ 9 та програмних результатів навчання: ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9-13, ПРН 17, ПРН 19, ПРН 33, ПРН 34, ПРН 44-46.</b></p>
<b>Ключові слова</b>	Штучний інтелект, інтелектуальна система, нейронна мережа, навчання, граф, пошук на графі, пошук вшир, пошук вглиб, евристики, алгоритм А*, нечіткі множини, експертні системи, ймовірність, робот, простір станів, знання, модель представлення

	знань.
<b>Формат курсу</b>	Очний. Проведення лекцій, лабораторних робіт і консультацій.
<b>Теми</b>	<ol style="list-style-type: none"> <li>1. Вступ. Поняття «штучний інтелект». Етапи розвитку штучного інтелекту. Штучний інтелект сьогодні. Соціальні мережі як елемент кіберпростору. Боти та штучний інтелект.</li> <li>2. Способи подання задач.</li> <li>3. Неінформовані методи пошуку.</li> <li>4. Інформовані методи пошуку в просторі станів.</li> <li>5. Подання задач у просторі підзадач. Графи AND/OR.</li> <li>6. Методи подання знань. Логічні моделі.</li> <li>7. Продукційна, семантична та фреймова моделі представлення знань.</li> <li>8. Поняття про експертні системи підтримки прийняття рішень.</li> <li>9. Вступ до нейроінформатики.</li> <li>10. Саморганізаційні та інші види мереж. Гібридні мережі.</li> <li>11. Нечітке моделювання.</li> <li>12. Задачі кібербезпеки. Можливі напрямки застосування штучного інтелекту у кібербезпеці.</li> </ol>
<b>Підсумковий контроль, форма</b>	Екзамен у кінці шостого семестру.
<b>Пререквізити</b>	Для вивчення дисципліни студенти потребують базові знання з курсу "Застосування дискретної математики в криптології", "Моделі та методи дискретної математики", "Застосування теорії ймовірності в кібербезпеці", "Обробка сигналів в кібербезпеці", "Прикладна статистика".
<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	Презентації, лекції Індивідуальні завдання Групові проекти, менторство
<b>Необхідне обладнання</b>	Комп'ютер, Internet.
<b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• поточне опитування: 40% семестрової оцінки; максимальна кількість балів 40;</li> <li>• індивідуальне завдання: 10% семестрової оцінки; максимальна кількість балів 10;</li> <li>• іспит: 50% семестрової оцінки; максимальна кількість балів 50.</li> </ul> <p>Підсумкова максимальна кількість балів 100.</p> <p><b>Лабораторні роботи:</b> Очікується, що студенти виконають чотири лабораторних роботи і одне індивідуальне завдання.</p> <p><b>Академічна доброчесність:</b> Очікується, що роботи студентів будуть їх самостійними дослідженнями чи міркуваннями. 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.</p> <p><b>Відвідування занять</b> є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні</p>

	<p>заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів, визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.</p> <p><b>Література.</b> Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p><b>Політика виставлення балів.</b> Враховуються бали, отримані при поточному опитуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнь на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях, не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p>
<p><b>Питання до екзамену.</b></p>	<p>Поняття «штучний інтелект». Етапи розвитку штучного інтелекту.</p> <p>Штучний інтелект сьогодні. Соціальні мережі як елемент кіберпростору. Боти та штучний інтелект.</p> <p>Способи подання задач і пошук розв'язків.</p> <p>Модель предметної області. Простір станів.</p> <p>Методи "сліпого пошуку". Методи пошуку вшир і вглиб.</p> <p>Алгоритм рівних цін.</p> <p>Евристичні методи пошуку в просторі станів. Алгоритм пошуку по першому найкращому збігу, A-алгоритм. Алгоритм "підйому на гору".</p> <p>Виявлення шахрайства за допомогою алгоритмів пошуку на графах.</p> <p>Подання задач у просторі підзадач. Графи AND/OR.</p> <p>Дані та знання. Декларативні знання та процедурні.</p> <p>Логічна модель представлення знань.</p> <p>Продукційна, семантична та фреймова моделі представлення знань.</p> <p>Поняття про експертні системи підтримки прийняття рішень. Їх призначення, класифікація, структура. Дерево рішень.</p> <p>Приклади експертних систем з питань кібербезпеки.</p> <p>Нейронні мережі. Персептрон і його розвиток.</p> <p>Багатошаровий персептрон і алгоритм зворотного поширення помилки.</p> <p>Саморганізаційні та радіально-базисні нейронні мережі. Гібридні мережі.</p> <p>Виявлення аномалій в мережі, що може свідчити про вторгнення або інші загрози.</p> <p>Нечіткі множини. Операції з нечіткими множинами.</p> <p>Нечіткі числа та операції з ними. Нечіткі відношення.</p> <p>Задачі кібербезпеки. Можливі напрямки застосування штучного інтелекту у кібербезпеці.</p>
<p><b>Опитування</b></p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенні курсу.</p>

Ти ж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання, год	Термін виконання
1	<b>Тема 1. Вступ. Поняття «штучний інтелект». Етапи розвитку штучного інтелекту.</b>	Лекція, самостійна	[1-9]	2, 4	1 тиждень
	<b>Тема 1. Вступ. Поняття «штучний інтелект». Штучний інтелект сьогодні. Соціальні мережі як елемент кіберпростору. Боти та штучний інтелект.</b>	Лабораторна	[1-9]	2	1 тиждень
2	<b>Тема 2. Способи подання задач.</b> Модель предметної області. Простір станів. Подання задачі в просторі станів.	Лекція, самостійна	[1-9]	2, 4	1 тиждень
	<b>Тема 2. Подання задачі в просторі станів.</b>	Лабораторна		2	1 тиждень
3	<b>Тема 3. Неінформовані методи пошуку.</b> Методи пошуку вшир і вглиб. Алгоритм рівних цін.	Лекція, самостійна	[1-9]	2, 4	1 тиждень
	<b>Тема 3. Неінформовані методи пошуку.</b> Методи пошуку вшир і вглиб. Алгоритм рівних цін.	Лабораторна	[1-9]	2	1 тиждень
4	<b>Тема 4. Інформовані методи пошуку в просторі станів.</b> Алгоритм пошуку по першому найкращому збігу, A-алгоритм, алгоритм "підйому на гору".	Лекція, самостійна	[1-9]	2, 4	1 тиждень
	<b>Тема 4. Інформовані методи пошуку в просторі станів.</b> Алгоритм пошуку по першому найкращому збігу, A-алгоритм, алгоритм "підйому на гору". Виявлення шахрайства за допомогою алгоритмів пошуку на графах.	Лабораторна	[1-9]	2	1 тиждень
5-6	<b>Тема 5. Подання задач у просторі підзадач. Графи AND/OR.</b>	Лекція Самостійна	[1-9]	4 6	2 тижні
	<b>Тема 5. Подання задач у просторі підзадач. Графи AND/OR.</b> Пошук вшир та вглиб на I/АБО графах.	Лабораторна	[1-9]	2	1 тиждень
	<b>Модульний контроль</b>	Лабораторна	[1-9]	2	1 тиждень
7	<b>Тема 6. Методи подання знань. Логічні моделі.</b> Основи логіки предикатів: синтаксис та семантика. Метод резолюцій Робінсона.	Лекція Самостійна	[1-9]	2 6	1 тиждень

	<b>Тема 6. Методи подання знань. Логічні моделі.</b> Дані та знання. Створення індивідуальної БЗ з використанням різних моделей подання знань.	Лабораторна	[1-9]	2	1 тиждень
8	<b>Тема 7. Продукційна, семантична та фреймова моделі подання знань.</b>	Лекція Самостійна	[1-9]	2 6	1 тиждень
	<b>Тема 7. Продукційна, семантична та фреймова моделі подання знань.</b> Створення індивідуальної БЗ з використанням різних моделей подання знань.	Лабораторна	[1-9]	2	1 тиждень
9-10	<b>Тема 8. Поняття про експертні системи.</b> Характеристики та етапи побудови експертних систем. Области застосування та види експертних систем. Перспективи розвитку експертних систем.	Лекція Самостійна	[1-9]	4 6	2 тижні
	<b>Тема 8. Експертні системи підтримки прийняття рішень.</b> Приклади експертних систем з питань кібербезпеки. Створення індивідуальної експертної системи на основі дерева рішень.	Лабораторна	[1-9]	4	2 тижні
11-13	<b>Тема 9. Вступ до нейроінформатики.</b> Перцептрон і його розвиток. Математичний нейрон Мак-Каллока-Пітса. Перцептрон Розенблатта і правила Гебба. Дельта-правило і розпізнавання букв. Обмеженість одношарового перцептрона. Багатошаровий перцептрон і алгоритм зворотного поширення помилки.	Лекція Самостійна	[1-9]	6 10	3 тижні
	<b>Тема 9. Вступ до нейроінформатики.</b> Створення нейромережі, що розпізнає букви українського та грецького алфавітів.	Лабораторна	[1-9]	6	3 тижні
14	<b>Тема 10. Саморганізаційні та інші види мереж. Гібридні мережі.</b> Виявлення аномалій в мережі, що може свідчити про вторгнення або інші загрози.	Лекція Самостійна	[1-9]	2 2	1 тиждень
	Створення нейромережі, що розпізнає букви українського та грецького алфавітів.	Лабораторна	[1-9]	2	1 тиждень
15	<b>Тема 11. Нечітке моделювання.</b> Нечіткі множини. Операції з нечіткими множинами. Нечіткі числа.	Лекція Самостійна	[1-9]	2 2	2 тижні
	<b>Тема 11. Нечітке моделювання.</b> Операції з нечіткими множинами	Лабораторна	[1-9]	2	1 тиждень

	та нечіткими числами.				
16	<b>Тема 12. Задачі кібербезпеки. Можливі напрямки застосування штучного інтелекту у кібербезпеці.</b>	Лекція Самостійна	[1-9]	2 2	1 тиждень
	<b>Модульний контроль.</b>	Лабораторна	[1-9]	2	1 тиждень