**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.**

| | |
|---|---|
| **Назва дисципліни** | **Системи штучного інтелекту** |
| **Адреса викладання дисципліни** | Головний корпус ЛНУ ім. І. Франка<br>м. Львів, вул. Університетська 1 |
| **Факультет та кафедра, за якою закріплена дисципліна** | Факультет прикладної математики та інформатики<br>кафедра кібербезпеки |
| **Галузь знань, шифр та назва спеціальності** | 12 – інформаційні технології<br>125 – кібербезпека та захист інформації |
| **Викладачі дисципліни** | Пелешко Дмитро Дмитрович, професор кафедри кібербезпеки<br>Колос Надія Мирославівна, доцент кафедри дискретного аналізу та інтелектуальних систем. |
| **Контактна інформація викладачів** | dmytro.peleshko@lnu.edu.ua<br>nadiya.kolos@lnu.edu.ua<br>Головний корпус ЛНУ ім. І. Франка<br>м. Львів, вул. Університетська, 1 |
| **Консультації з питань навчання по дисципліні відбуваються** | Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю). |
| **Сторінка курсу** | https://ami.lnu.edu.ua/academics/bachelor |
| **Інформація про дисципліну** | 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). |
| **Коротка анотація дисципліни** | 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. |
| **Мета та цілі дисципліни** | Метою даного курсу є ознайомити студентів з основними підходами до вирішення інтелектуальних задач; сформувати освоєння основних принципів побудови та функціонування інтелектуальних систем; виробити навички та вміння по вибору методів та алгоритмів для вирішення типових інтелектуальних задач.<br>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. |
| **Література для вивчення дисципліни** | **Основна література:**<br>1. Булгакова О.С., Зосімов В.В., Поздєєв В.О. Методи та системи штучного інтелекту: теорія та практика, - Вид-во Гельветика, 2020. – 356 ст.<br>2. Artificial Intelligence. A Modern Approach. (4th Edition). Stuart J. Russell and Peter Norvig. – 4d ed., - Pearson Education, 2020/ - 1136 p.<br>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. |

| | |
|---|---|
| | 4. Троцько В.В. Методи штучного інтелекту: навчально-методичний і практичний посібник, К.: Університет "КРОК", 2020. – 86 с.<br>5. Шаповал Н.В. Методи та системи штучного інтелекту. Комп'ютерний практикум [Електронний ресурс], - КПІ ім. Ігоря Сікорського, 2022. – 44 ст. - https://ela.kpi.ua/bitstream/123456789/57162/1/Shapoval_SMShI.pdf<br>**Додаткова література:**<br>1. Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина, Системи штучного інтелекту, Львів, 2010.<br>2. Савченко А.С., Синельніков О.О. Методи та системи штучного інтелекту – К. : НАУ, 2017. – 190 с.<br>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.<br>4. Haykin S. Neural networks and learning machines / Simon Haykin.—3rd ed. Pearson, 2018. – 938 с. |
| **Обсяг курсу** | Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 години лабораторних занять. Самостійної роботи: 56 годин. |
| **Очікувані результати навчання** | Після завершення цього курсу студент буде:<br>• ***знати:***<br>– основні методи використання технологій штучного інтелекту для задач кібербезпеки<br>– формулювання основних понять і означень штучного інтелекту;<br>– способи подання задач і методи пошуку розв'язків;<br>– базові концепції та загальну характеристику інтелектуальних систем;<br>– основні класичні підходи до вирішення типових інтелектуальних задач;<br>– основи моделювання та представлення знань (фреймові, семантичні логічні моделі);<br>– основи формалізації експертних знань та основні принципи створення та функціонування експертних систем.<br>• ***вміти***:<br>– використовувати технології штучного інтелекту для задач кібербезпеки<br>– формалізувати знання за допомогою різних способів представлення знань;<br>– розробляти модульну інтелектуальну систему на модельному та концептуальному рівні;<br>– проектувати інтелектуальні системи, експертні системи, бази знань;<br>– використовувати інтелектуальні системи для вирішення прикладних завдань у кібербезпеці.<br>**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.** |
| **Ключові слова** | 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. |
| **Формат курсу** | Очний.<br>Проведення лекцій, лабораторних робіт і консультацій. |
| **Теми** | 1. Вступ. Поняття «штучний інтелект». Етапи розвитку штучного інтелекту. Штучний інтелект сьогодні. Соціальні мережі як елемент кіберпростору. Боти та штучний інтелект.<br>2. Способи подання задач.<br>3. Неінформовані методи пошуку.<br>4. Інформовані методи пошуку в просторі станів.<br>5. Подання задач у просторі підзадач. Графи AND/OR.<br>6. Методи подання знань. Логічні моделі.<br>7. Продукційна, семантична та фреймова моделі представлення знань.<br>8. Поняття про експертні системи підтримки прийняття рішень.<br>9. Вступ до нейроінформатики.<br>10. Саморганізаційні та інші види мереж. Гібридні мережі.<br>11. Нечітке моделювання.<br>12. Задачі кібербезпеки. Можливі напрямки застосування штучного інтелекту у кібербезпеці. |
| **Підсумковий контроль, форма** | Екзамен у кінці шостого семестру. |
| **Пререквізити** | 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". |
| **Навчальні методи та техніки, які будуть використовуватися під час викладання курсу** | Презентації, лекції<br>Індивідуальні завдання<br>Групові проекти, менторство |
| **Необхідне обладнання** | Комп’ютер, Internet. |
| **Критерії оцінювання (окремо для кожного виду навчальної діяльності)** | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:<br>• поточне опитування: 40% семестрової оцінки; максимальна кількість балів 40;<br>• індивідуальне завдання: 10% семестрової оцінки; максимальна кількість балів 10;<br>• іспит: 50% семестрової оцінки; максимальна кількість балів 50.<br>Підсумкова максимальна кількість балів 100.<br>**Лабораторні роботи:** Очікується, що студенти виконають чотири лабораторних роботи і одне індивідуальне завдання.<br>**Академічна доброчесність**: 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.<br>**Відвідування занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні |

| | |
|---|---|
| | 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.<br>**Література.** 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.<br>**Політика виставлення балів.** 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 запізнень 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.<br>Жодні форми порушення академічної доброчесності не толеруються. |
| **Питання до екзамену.** | Поняття «штучний інтелект». Етапи розвитку штучного інтелекту.<br>Штучний інтелект сьогодні. Соціальні мережі як елемент кіберпростору. Боти та штучний інтелект.<br>Способи подання задач і пошук розв'язків.<br>Модель предметної області. Простір станів.<br>Методи "сліпого пошуку". Методи пошуку вшир і вглиб. Алгоритм рівних цін.<br>Евристичні методи пошуку в просторі станів. Алгоритм пошуку по першому найкращому збігу, А-алгоритм. Алгоритм "підйому на гору".<br>Виявлення шахрайства за допомогою алгоритмів пошуку на графах.<br>Подання задач у просторі підзадач. Графи AND/OR.<br>Дані та знання. Декларативні знання та процедурні.<br>Логічна модель представлення знань.<br>Продукційна, семантична та фреймова моделі представлення знань.<br>Поняття про експертні системи підтримки прийняття рішень. Їх призначення, класифікація, структура. Дерево рішень.<br>Приклади експертних систем з питань кібербезпеки.<br>Нейронні мережі. Персептрон і його розвиток.<br>Багатошаровий персептрон і алгоритм зворотного поширення помилки.<br>Саморганізаційні та радіально-базисні нейронні мережі. Гібридні мережі.<br>Виявлення аномалій в мережі, що може свідчити про вторгнення або інші загрози.<br>Нечіткі множини. Операції з нечіткими множинами.<br>Нечіткі числа та операції з ними. Нечіткі відношення.<br>Задачі кібербезпеки. Можливі напрямки застосування штучного інтелекту у кібербезпеці. |
| **Опитування** | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенні курсу. |

Схема курсу

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

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

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