Силабус освітнього компонента
Програма навчальної дисципліни

Математичні основи штучного інтелекту

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
5

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Курс "Математичні основи штучного інтелекту" охоплює базові математичні концепції та методи, що лежать в основі сучасних алгоритмів і систем штучного інтелекту (ШІ). Студенти вивчатимуть такі області як лінійна алгебра, ймовірність і статистика, математичний аналіз, оптимізація та теорія графів, які є необхідними для розуміння алгоритмів машинного навчання, нейронних мереж, прийняття рішень і обробки даних. Лабораторні заняття допомагають студентам закріпити отримані знання на практиці.

Мета та цілі дисципліни

Метою навчальної дисципліни " Математичні основи штучного інтелекту ", є забезпечення студентів теоретичними та практичними знаннями з математичних основ, необхідних для розуміння та розробки методів і алгоритмів штучного інтелекту.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ–2. Знання та розуміння предметної області та розуміння професії.
КЗ–5. Здатність до пошуку, оброблення та аналізу інформації.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Результати навчання

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Основи математичного моделювання систем безпеки.

Особливості дисципліни, методи та технології навчання

Викладання дисципліни передбачає використання пояснювально-ілюстративного та репродуктивного методів, а також активізацію навчально-пізнавальної діяльності через презентації, індивідуальні та групові проекти, моделювання систем, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до математичних методів у штучному інтелекті.
Огляд ключових математичних розділів, що застосовуються в ШІ. Роль математики у розробці моделей машинного навчання
Тема 2. Лінійна алгебра для штучного інтелекту.
Вектори, матриці, операції над ними. Власні вектори, власні значення, сингулярний розклад матриць (SVD).
Тема 3. Ймовірність і статистика у ШІ.
Основи ймовірнісних розподілів. Умовні ймовірності, Байєсівські мережі, закони великих чисел
Тема 4. Теорія прийняття рішень на основі ймовірностей.
Теорія Байєса та її застосування у ШІ. Прогнозування на основі ймовірнісних моделей
Тема 5. Математичний аналіз та його застосування у ШІ.
Похідні, градієнти, інтеграли. Градієнтний спуск: основи та модифікації (стохастичний, міні-батч) Методи моделювання. Інструменти для симуляції. Прикладні задачі моделювання.
Тема 6. Теорія графів та алгоритми на графах.
Базові поняття графів: вершини, ребра, ступені. Алгоритми пошуку на графах та їх використання у штучному інтелекті
Тема 7. Чисельні методи у задачах ШІ.
Основи чисельної лінійної алгебри. Методи для розв'язування лінійних систем та найменших квадратів
Тема 8. Математичні основи оптимізації.
Задачі оптимізації у машинному навчанні. Градієнтний спуск та методи прискорення оптимізації (метод Ньютона, моментум)
Тема 9. Методи регуляризації у машинному навчанні.
L1 та L2 регуляризація. Проблема перенавчання та боротьба з ним за допомогою регуляризації
Тема 10. Основи теорії інформації та ентропії.
Визначення інформації та ентропії. Крос-ентропія, дивергенція Кульбака-Лейблера та їх використання в алгоритмах ШІ.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1 Основи роботи з лінійною алгеброю.
Операції з векторами та матрицями. Власні значення та розклади матриць.
Тема 2. Моделювання випадкових подій за допомогою ймовірнісних методів.
Розрахунок умовних ймовірностей. Реалізація Байєсівських мереж
Тема 3. Градієнтний спуск.
Реалізація градієнтного спуску для задачі мінімізації. Вивчення варіантів алгоритму (стохастичний, міні-батч)
Тема 4. Оптимізаційні методи.
Практичне застосування методів оптимізації в задачах навчання моделей. Реалізація алгоритмів пошуку мінімуму
Тема 5 Чисельні методи.
Вирішення задач за допомогою методу найменших квадратів. Чисельні методи для розв'язування систем лінійних рівнянь.
Тема 6 Моделювання на графах.
Реалізація базових алгоритмів на графах. Візуалізація та аналіз графових структур

Тема 7 Практика побудови нейронної мережі.
Побудова простої нейронної мережі з використанням бібліотек (наприклад, TensorFlow, PyTorch)
Навчання моделі та аналіз результатів
Тема 8 Кластеризація та регресія.
Реалізація алгоритмів кластеризації та регресії на реальних даних. Оцінка та візуалізація результатів моделі.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта
В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Глибовець А. М., Гулаєва Н. М. Еволюційні алгоритми. М. - К.: НаУКМА, 2013., 828с. URL:
2. Кононюк А.Ю. Нейроні мережі і генетичні алгоритми – К.:«Корнійчук», 2008. – 446 с. URL: https://pdf.lib.vntu.edu.ua/books/2016/Kononyk_2008_470.pdf
3. Математичний апарат штучного інтелекту в електроенергетичних системах: підручник / В.В.Кирик. - Київ: КПІ ім. Ігоря Сікорського, вид-во "Політехніка". - 2019.-224 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/34259dab-7eaa-4b78-86d9-4a000d90b2be/content

Додаткова література

1. Литвин, В.В. Інтелектуальні системи / В.В. Литвин. - Львів: Новий світ-2000. - 2009. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Intelektual_system.pdf
2. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» / Уклад. : А.С. Савченко, О. О. Синельніков. – К. : НАУ, 2017. – 190с. URL: https://er.nau.edu.ua/bitstream/NAU/40676/1/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%20%D1%82%D0%B0%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8%20%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83%20_%D0%9D%D0%B0%D0%B2%D1%87_%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD.pdf
3. Руденко О. Г., Бодянський Є. В. Штучні нейронні мережі: Навчальний посібник. — Харків: ТОВ "Компанія СМІТ", 2006. — 404 с. URL: https://f.eruditor.link/file/260293/
4. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень. Запоріжжя: ЗНТУ, 2008. — 341 с. URL: https://eir.zp.edu.ua/server/api/core/bitstreams/63742fdf-b5e4-46e2-83b4-561d97c2cffe/content.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено 28.08.2024 Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 Гарант ОП
Сергій ЄВСЕЄВ