Навчальна дисципліна

Методи штучного інтелекту для кібербезпеки

Галузі знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 16 «Хімічна інженерія та біоінженерія», 17 «Електроніка, автоматизація та електронні комунікації», 19 «Архітектура та будівництво», 27 «Транспорт» (спеціальність 272 Авіаційний транспорт)

Рівень вищої освіти	*другий (магістерський)*
Статус дисципліни	*вибіркова*
Обсяг дисципліни	150 годин/ 5кредитів ЄКТС
Мова викладання	*українська*
Анотація	Курс «Методи штучного інтелекту для кібербезпеки» дозволяє вивчити практичні приклади сумісного використання систем штучного інтелекту і баз знань у різних галузях (охорона здоров'я, промисловість, безпека, фінансовий сектор, енергетика тощо) та особливості реалізації галузево-орієнтованих проектів для систем кібербезпеки щодо машинного навчання, автоматичного доведення та інтроспекції. Значну увагу приділено існуючим технологіям розробки безпечних баз знань для систем штучного інтелекту. Представлено універсальну систему розробки корпоративної бази знань Zendesk Guide, існуючі підходи до формування баз знань для Deep Learning в системах штучного інтелекту та декілька фреймворків Python. Зокрема, розглядаються такі фреймворки як основний бекенд для обчислень при розпізнаванні зображень системами щтучного інтелекту (СШІ) – Tensorflow, фреймворк для побудови нейронних мереж, що підтримує основні види шарів і структурні елементи – Keras, фреймворки для опрацювання онтологій баз знань та градієнтного бустінга – NLTK, Gensim, Xgboost, LightGBM, CatBoost. Роглянуто засоби аналізу і забезпечення кібербезпеки систем штучного інтелекту на сучасних принципах Trustworthy AI. Освоєння курсу дозволить опанувати базові знання щодо підготовки та реалізації проекту галузево-орієнтованої безпечної системи штучного інтелекту з базою знань для Deep Learning. **Мета** курсу – засвоєння необхідних знань, навичок та вмінь з вибору та реалізації методів побудови безпечних СШІ та формування баз знань під час реалізації проекту галузево-орієнтованої безпечної системи штучного інтелекту з базою знань для Deep Learning. **Завдання** дисципліни – навчити студентів формувати завдання, аналізувати вимоги до кібербезпеки, створювати команду, розподіляти ролі та виконувати галузево-орієнтовані проекти СШІ з базою знань для Deep Learning з використанням фреймворків Python. У результаті навчання студент знатиме: – методи побудови СШІ та баз знань; – архітектуру СШІ з базою знань для Deep Learning; – фреймворки Python для побудови СШІ та онтологій баз знань; – вимоги до безпеки СШІ; вмітиме: – розробляти архітектуру СШІ з базою знань для Deep Learning; – формувати команду та розподіляти обов'язки для реалізації проекту галузево-орієнтованої системи штучного інтелекту з базою знань для Deep Learning; – розгортати та ефективно застосовувати фреймворки Python відповідно до задач проекту СШІ з базою знань для Deep Learning та його галузевої специфіки; – забезпечувати кібербезпеку СШІ; **матиме компетентності**: – здатність ефективно використовувати основні методи побудови безпечних СШІ та баз знань; – здатність розгортати та ефективно застосовувати фреймворки Python для побудови СШІ та онтологій баз знань у відповідному середовищі з урахуванням вимог до безпеки; – здатність реалізовувати ефективну політику щодо забезпечення конфіденційності корпоративних даних;

<table>
<tr><td></td><td colspan="3">– здатність ефективно працювати у складі команди щодо виконання проекту ШІ з базою знань для Deep Learning.
Особливості курсу:
– практична спрямованість і кейс-орієнтований підхід при викладанні;
– надає комплекс знань, практичних навичок і компетентностей, достатніх для подальшого самостійного вивчення і застосування для практичної діяльності;
– побудований з урахуванням досвіду провідних університетів (зокрема, Massachusetts Institute of Technology) і потреб провідних IT-компаній (зокрема, EPAM, NIX Solutions), а також стандартів і методичних матеріалів NIST (National Institute of Standards and Technology, USA);
– розроблений і викладається фахівцем, який має досвід у галузі систем штучного інтелекту, зокрема, виконання низки індустріальних проєктів, пов’язаних з моніторингом лісових пожеж, виявлення бурштинових копалин, розпізнаванням облич, технологіями доповненої реальності тощо</td></tr>
<tr><td>Організація навчання</td><td colspan="3">Види занять: лекції, лабораторні заняття.
Форми здобуття освіти: денна, заочна.
Форми контролю: модульний контроль, іспит</td></tr>
<tr><td>Кафедра</td><td colspan="3">Кафедра комп'ютерних систем, мереж і кібербезпеки</td></tr>
<tr><td>Факультет</td><td colspan="3">Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій</td></tr>
<tr><td>Викладач</td><td>  </td><td>ПІБ</td><td>Кучук
Георгій Анатолійович</td></tr>
<tr><td></td><td></td><td>Посада</td><td>професор</td></tr>
<tr><td></td><td></td><td>Вчене звання</td><td>професор</td></tr>
<tr><td></td><td></td><td>Науковий ступінь</td><td>доктор технічних наук</td></tr>
<tr><td></td><td></td><td>e-mail</td><td></td></tr>
<tr><td>Посилання на електронні матеріали курсу</td><td colspan="3">https://mentor.khai.edu/course/view.php?id=8281</td></tr>
<tr><td>Посилання на робочу програму (силабус)</td><td colspan="3">https://khai.edu/assets/files/silabusi/dp4/504_rp_metodi-shtuchnogo-intelektu-dlya-kiberbezpeki.pdf</td></tr>
</table>