WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI/KATEDRA PODSTAW INFORMATYKI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim : **Uczenie Maszynowe - Prywatność i Bezpieczeństwo**
Nazwa przedmiotu w języku angielskim : **Machine Learning - Privacy and Security**
Kierunek studiów : **Informatyka algorytmiczna**
Specjalność (jeśli dotyczy) : **—**
Poziom i forma studiów : **II stopień, stacjonarna**
Rodzaj przedmiotu : **wybieralny**
Język wykładowy : **polski**
Cykl kształcenia od : **2023/2024**
Kod przedmiotu : **W04INA-SM0135G**
Grupa zajęć : **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2		3		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2.72				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Zastosowanie uczenia maszynowego (ML) do wykrywania anomalii i zagrożeń w systemach informatycznych. Przegląd wykrywania ataków sieciowych w oparciu o ML. Przedstawienie podstawowych zagrożeń związanych z procesem ML. Omówienie technik zapewniających integralność wejść i wyjść procesu ML. Przegląd mechanizmów zapewniających prywatność i poufność uczenia maszynowego wdrażanych na platformach zdalnych. Omówienie problemu możliwego do udowodnienia zdalnego treningu w procesach ML.

C2 Wdrożenie wybranych technik wykrywania anomalii w oparciu o uczenie maszynowe (ML). Implementacja wybranych metod zapewniających prywatność i poufność procesów ML.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy studenta:

W1 Zastosowanie ML w wykrywaniu anomalii i zagrożeń w systemach IT.

W2 Świadomość zagrożeń i podatności związanych z procesem ML.

W3 Ochrona procesów ML.

Z zakresu umiejętności studenta:

U1 Kursant umie stosować wybrane techniki ML do wykrywania anomalii i zagrożeń w systemach IT.

U2 Kursant umie identyfikować zagrożenia i podatności związane z procesem ML.

U3 Kursant potrafi zarządzać ochroną procesów ML.

Z zakresu kompetencji społecznych studenta:

K1 Kursant potrafi określić bezpieczeństwo rozwiązań ML w kontekście gospodarczym i społecznym.

K2 Kursant potrafi zidentyfikować potencjalne obszary zastosowań uczenia maszynowego w kontekście gospodarczym i społecznym.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Wprowadzenie do ML.	4h
Wy2	Wykrywanie anomalii i zagrożeń w oparciu o ML.	4h
Wy3	ML na zdalnych platformach (w chmurach obliczeniowych).	4h
Wy4	Tajność danych w procesach ML.	3h
Wy5	Prywatność w ML.	3h
Wy6	Spójność danych treningowych, błędne etykietowanie.	3h
Wy7	Dowodliwy ML, dowodliwy proces treningu.	3h
Wy8	Bezpieczny rozproszony ML.	3h
Wy9	Bezpieczny ML z szyfrowaniem homomorficznym	3h
	Suma godzin	30h

Forma zajęć - laboratorium		
Lab1	Wprowadzenie do ML.	6h
Lab2	Wykrywanie anomalii i zagrożeń w oparciu o ML.	6h
Lab3	Spójność danych treningowych i błędne etykietowanie.	6h
Lab4	Prywatność i tajność w ML.	6h
Lab5	Dowodliwy ML, dowodliwy proces treningu ML.	6h
	Suma godzin	30h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Wykład multimedialny
3. Rozwiązywanie zadań programistycznych
4. Tworzenie projektów programistycznych
5. Konsultacje
6. Praca własna studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F - formatująca (w trakcie semestru), P - podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	W1-W3, K1-K2	Aktywność
F2	U1-U3, K1-K2	Średnia ocen z list zadań laboratoryjnych.
P=20%*F1+80%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Publikacje z zakresu bezpieczeństwa ML wskazane przez prowadzącego zajęcia.

NAUCZYCIEL AKADEMICKI ODPOWIEDZIALNY ZA PRZEDMIOT

dr hab. inż. Łukasz Krzywiecki

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA SIĘ DLA PRZEDMIOTU
Uczenie Maszynowe - Prywatność i Bezpieczeństwo
Z EFEKTAMI UCZENIA SIĘ NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się zdefiniowanych dla kierunku studiów	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K2_W01 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07	C1	Wy1-Wy9	1 2 5 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W07	C1	Wy1-Wy9	1 2 5 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07	C1	Wy1-Wy9	1 2 5 6
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K08 K2_K10 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5 6
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K08 K2_K10 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5 6