Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Metody sztucznej inteligencji w cyberbezpieczeństwie
Nazwa przedmiotu w języku angielskim	Artificial Intelligence Methods in Cybersecurity
Kod przedmiotu	WIiT I oIIN D7 23/24
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	9	0	0	0	0	18

3 Cele przedmiotu

Cel 1 Przekazanie studentom podstawowej wiedzy na temat zagrożeń w systemach informatycznych i metodach ich wykrywania i eliminacji z wykorzystaniem nowoczesnych metod sztucznej inteligencji.

Cel 2 Zdobycie przez studentów doświadczenia w prostych pracach projektowych dotyczących implementacji nowoczesnych systemów IDS opartych na metodach uczenia maszynowego.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Podstawowe informacje dotyczące baz danych i programowania (preferowany Python).

2 Podstawy bezpieczeństwa w systemach informatycznych.

5 Efekty kształcenia

EK1 Wiedza Znajomość podstawowych modeli wykrywania zagrożeń w ruchu sieciowym i anomalii w zbiorach danych.

EK2 Umiejętności Umiejętność zdefiniowania założeń projektowych (problem, metoda), zebranie i wstępna obróbka danych, wybór odpowiednich narzędzi implementacyjnych.

EK3 Umiejętności Umiejętność implementacji algorytmów sztucznej inteligencji do wykrywania ataków i anomalii w systemach informatycznych, wykonanie eksperymentów numerycznych.

EK4 Kompetencje społeczne Świadomość znaczenia praktycznego nowoczesnych algorytmów wykrywania zagrożeń w ruchu sieciowym i detekcji anomalii w zbiorach danych, umiejętność pracy w zespołach projektowych.

6 Treści programowe

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Definicja problemu np. wykrywanie sygnatur ataków DDoS, wykrywanie anomalii w ruchu sieciowym, wykrywanie anomalii w danych, etc. Podział na grupy projektowe, opracowanie planu pracy i harmonogramu wykonania zadań.	2
P2	Definicja metody (metod) rozwiązania postawionego problemu, wybór repozytoriów danych testowych, wstępna obróbka danych, pierwszy etap projektu, początkowe rozdziały sprawozdania.	4
P3	Wybór narzędzi i implementacja wybranych metod zapoznanie się z bibliotekami i użytecznymi frameworkami w Python (Keras, Scikit-learn, etc.) zakończenie II etapu pisania sprawozdania.	6
P4	Wykonanie eksperymentów i dokończenie sprawozdania.	4
P5	Prezentacja projektów.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wprowadzenie do przedmiotu, podstawowe klasy i ewolucja metod sztucznej inteligencji, uczenie maszynowe.	1

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W2	Rodzaje zagrożeń monitoring ruchu sieciowego, pre-processing danych, metody adaptacji.	2
W3	Metody wykrywania ataków w ruchu sieciowym: podejście sygnaturowe i wykrywanie anomalii, IDS (systemy wykrywania ataków sieciowych, ang. Intrusion Detection Systems) oparte na metodach sztucznej inteligencji wprowadzenie.	3
W4	Zastosowanie metod uczenia maszynowego w IDS.	2
W5	Miary skuteczności metod a systemach IDS.	1

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Konsultacje, Dyskusja

N3 Prezentacje multimedialne

N4 Ćwiczenia projektowe

N5 Praca zdalna - wykorzystanie MS TEAMS i/lub DELTA

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	27
Konsultacje przedmiotowe	15
Egzaminy i zaliczenia w sesji	0
konsultacje indywidualne na platformie TEAMS	18
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
Sumaryczna liczba punktów ECTS dla przedmiotu	3.00

9 Sposoby oceny

Nie przeprowadza się testu wprowadzającego.

Ocena formująca

F1 Sprawozdania z wykonanych projektów.

F2 Prezentacja wyników pracy w projektach.

Ocena podsumowująca

P1 Średnia ważona ocen formujących (85%, 15%).

Warunki zaliczenia przedmiotu

W1 Pozytywna ocena z ćwiczeń projektowych - zaliczenie wszystkich elementów.

W2 Brak nieusprawiedliwionych nieobecności na obowiązkowych formach zajęć

Ocena aktywności bez udziału nauczyciela

B1 Ocena pracy indywidualnej studenta nad wykonaniem projektu - ocena raportów z postępów pracy wysyłanych prowadzącym zajęcia i prezentowanych podczas zajęć (również z wykorzystywaniem metod nauczania zdalnego).

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia wymagań na ocenę 3.0.
Na ocenę 3.0	Student zna ogólne zasady dotyczących zagrożeń w systemach informatycznych, potrafi sklasyfikować te zagrożenia i uzasadnić stosowanie metod sztucznej inteligencji do ich detekcji.
Na ocenę 3.5	Student zna ogólne zasady dotyczących zagrożeń w systemach informatycznych, potrafi dokonać wszechstronnej analizy tych zagrożeń, sklasyfikować je i uzasadnić stosowanie metod sztucznej inteligencji do ich detekcji.
Na ocenę 4.0	Student zna i potrafi scharakteryzować i sklasyfikować zagrożenia w systemach informatycznych, zna podstawy nowoczesnych systemów IDS i potrafi uzasadnić stosowanie metod sztucznej inteligencji w tych systemach.
Na ocenę 4.5	Student zna i potrafi scharakteryzować i sklasyfikować zagrożenia w systemach informatycznych, zna strukturę i typy nowoczesnych systemów IDS i potrafi uzasadnić stosowanie metod sztucznej inteligencji w tych systemach.
Na ocenę 5.0	Student zna i potrafi dokonać wszechstronnej analizy i kompleksowej klasyfikacji zagrożeń w systemach informatycznych, zna nowoczesne systemy IDS oparte na metodach sztucznej inteligencji, potrafi zaproponować metody ich adaptacji do wykrywania konkretnego zagrożenia.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia wymagań na ocenę 3.0.
Na ocenę 3.0	Student potrafi zdefiniować prosty problem projektowy dotyczący detekcji anomalii lub ataków w sieciach informatycznych, dobrać metodę rozwiązania tego problemu, zebrać dane i wykonać ich wstępną obróbkę.
Na ocenę 3.5	Student potrafi zdefiniować prosty problem projektowy dotyczący detekcji anomalii lub ataków w sieciach informatycznych, dobrać metodę rozwiązania tego problemu, wybrać odpowiednie repozytorium z danymi testowymi, zebrać dane i wykonać ich wstępną obróbkę.
Na ocenę 4.0	Student potrafi zdefiniować złożony problem projektowy dotyczący detekcji anomalii lub ataków w sieciach informatycznych, dobrać metodę rozwiązania tego problemu, wybrać odpowiednie repozytorium z danymi testowymi, zebrać dane i wykonać ich wstępną obróbkę.
Na ocenę 4.5	Student potrafi zdefiniować złożony problem projektowy dotyczący detekcji anomalii lub ataków w sieciach informatycznych, dobrać 2-3 alternatywne metody rozwiązania tego problemu, wybrać odpowiednie repozytorium z danymi testowymi, zebrać dane i wykonać ich wstępną obróbkę.
Na ocenę 5.0	Student potrafi zdefiniować złożony problem projektowy dotyczący detekcji anomalii lub ataków w sieciach informatycznych, dobrać kilka alternatywnych metod rozwiązania tego problemu, potrafi wstępnie oszacować ich spodziewaną skuteczność, potrafi wybrać odpowiednie repozytorium z danymi testowymi, zebrać dane i wykonać ich wstępną obróbkę.

Efekt kształcenia 3	
Na ocenę 2.0	Student nie spełnia wymagań na ocenę 3.0.
Na ocenę 3.0	Student potrafi zaimplementować wskazane algorytmy detekcji ataków i anomalii w systemach informatycznych, przeprowadzić proste eksperymenty z wykorzystaniem zaimplementowanych algorytmów.
Na ocenę 3.5	Student potrafi zaimplementować wskazane algorytmy detekcji ataków i anomalii w systemach informatycznych, przeprowadzić proste eksperymenty z wykorzystaniem zaimplementowanych algorytmów, potrafi zinterpretować otrzymane wyniki.
Na ocenę 4.0	Student potrafi zaimplementować wskazane algorytmy detekcji ataków i anomalii w systemach informatycznych, przeprowadzić złożone testy jednostkowe wykonanego oprogramowania oraz eksperymenty numeryczne na dostarczonych danych testowych, potrafi zinterpretować wyniki tych testów.
Na ocenę 4.5	Student potrafi zaimplementować wskazane algorytmy detekcji ataków i anomalii w systemach informatycznych, przeprowadzić złożone testy jednostkowe wykonanego oprogramowania oraz eksperymenty numeryczne na dostarczonych danych testowych, potrafi zinterpretować wyniki tych testów za pomocą prostej analizy statystycznej.
Na ocenę 5.0	Student potrafi zaimplementować wskazane algorytmy detekcji ataków i anomalii w systemach informatycznych, przeprowadzić wszechstronną analizę eksperymentalną i dokonać zaawansowanej analizy statystycznej otrzymanych wyników.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia wymagań na ocenę 3.0.
Na ocenę 3.0	Student zna przynajmniej 1 przykład praktyczny metody opartej na AI wykrywania anomalii lub ataków DDoS w systemach informatycznych, wykonuje sumiennie zadania w zespole projektowym.
Na ocenę 3.5	Student zna kilka przykładów metod opartych na AI wykrywania anomalii lub ataków DDoS w systemach informatycznych, wykonuje sumiennie i terminowo zadania w zespole projektowym.
Na ocenę 4.0	Student zna kilka przykładów metod AI służących do wykrywania anomalii lub ataków DDoS w systemach informatycznych (sieciach komputerowych), potrafi je przedstawić w prosty sposób, wykonuje sumiennie i terminowo główne zadania w zespole projektowym.
Na ocenę 4.5	Student orientuje się w praktycznych zastosowaniach metod AI służących do wykrywania anomalii lub ataków DDoS w systemach informatycznych i potrafi wytłumaczyć zalety ich stosowania w praktyce, kieruje pracami zespołu projektowego.

Na ocenę 5.0	Student doskonale orientuje się w praktycznych zastosowaniach metod AI służących do wykrywania anomalii lub ataków DDoS w systemach informatycznych i potrafi wytłumaczyć zalety ich stosowania w praktyce na przykładach flagowych praktycznych projektów, kieruje pracami zespołu projektowego.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W02 I2_W05 I2_W06 I2_U01b I2_U05 I2_K01	Cel 1	W1 W2 W3 W4 W5	N1 N2 N3 N5	F2
EK2	I2_W02 I2_W03 I2_W06 I2_U02b I2_U03b I2_U04b I2_U05 I2_U07 I2_U08 I2_U11 I2_U12 I2_K01 I2_K02	Cel 1 Cel 2	P1 P2 P5 W2 W3 W4 W5	N1 N2 N3 N4 N5	F1 F2 P1
EK3	I2_W02 I2_W03 I2_W04 I2_U01b I2_U02b I2_U03b I2_U05 I2_U11 I2_K02 I2_K04	Cel 1 Cel 2	P2 P3 P5 W3 W4 W5	N2 N3 N4 N5	F1 F2 P1

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK4	I2_W02 I2_W03 I2_W05 I2_W06 I2_U01b I2_U02b I2_U03b I2_U11 I2_U12 I2_K01 I2_K02 I2_K03 I2_K04	Cel 1 Cel 2	P1 P2 P3 P4 P5 W3 W4 W5	N1 N2 N3 N4 N5	F1 F2 P1

11 Wykaz literatury

Literatura podstawowa

[1] **Emmanuel Tsukerman** — *Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python*, , 2019, Packt Publishing

Literatura uzupełniająca

[1] **Jerzy Surma** — *Hakowanie sztucznej inteligencji*, Warszawa, 2023, PWN

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr hab. prof.PK Joanna Kołodziej (kontakt: joanna.kolodziej@pk.edu.pl)

Osoby prowadzące przedmiot

1 dr hab. prof. PK Joanna Kołodziej (kontakt: joanna.kolodziej@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .