POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Wykrywanie anomalii w procesach, PG_00068082		
Kierunek studiów	Automatyka, cybernetyka i robotyka		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2028/2029
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć	Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	3	Język wykładowy	polski
Semestr studiów	6	Liczba punktów ECTS	2.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Systemów Decyzyjnych i Robotyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Mariusz Domżalski	
	Prowadzący zajęcia z przedmiotu	dr inż. Mariusz Domżalski	

Formy zajęć							
	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	15.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						

Aktywność studenta i liczba godzin pracy					
	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30	2.0	18.0	50

Cel przedmiotu	
	Celem przedmiotu jest zapoznanie studentów z teoretycznymi i praktycznymi aspektami wykrywania anomalii w danych procesowych i szeregach czasowych. Studenci poznają wachlarz metod od klasycznych technik statystycznych, przez algorytmy uczenia maszynowego, po zaawansowane modele głębokiego uczenia (sieci rekurencyjne, transformery). Kurs kładzie nacisk na praktyczne zastosowanie zdobytej wiedzy w rozwiązywaniu rzeczywistych problemów inżynierskich, takich jak predykcja awarii, monitoring systemów IoT czy analiza danych medycznych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W21] zna i rozumie podstawowe metody podejmowania decyzji oraz metody i techniki projektowania i eksploatacji systemów regulacji automatycznej i sterowania, zastosowania komputerów do sterowania i monitorowania systemów dynamicznych.	Zna i rozumie rolę oraz zastosowanie metod detekcji anomalii w kontekście monitorowania systemów dynamicznych, predykcyjnego utrzymania ruchu (predictive maintenance) i zapewniania bezpieczeństwa procesów.	[SW1] Ocena wiedzy faktograficznej
[K6_U04] potrafi wykorzystywać posiadaną wiedzę z zakresu metod i technik programowania oraz dobrać i zastosować właściwe metody i narzędzia programistyczne w tworzeniu oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo elementy lub układy programowalne, charakterystycznych dla danego kierunku studiów	Rozumie podstawy matematyczne i statystyczne leżące u podstaw omawianych metod detekcji anomalii, w tym koncepcje rozkładów prawdopodobieństwa, miar odległości oraz zasad optymalizacji stosowanych w modelach uczenia maszynowego.	[SU2] Ocena umiejętności analizy informacji [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu
[K6_W01] zna i rozumie w zaawansowanym stopniu matematykę w zakresie niezbędnym do formułowania i rozwiązywania prostych zagadnień związanych z kierunkiem studiów	Potrafi zaimplementować i przetestować wybrane algorytmy wykrywania anomalii (statystyczne, klastrowania, oparte na autoenkoderach) z wykorzystaniem dedykowanych bibliotek programistycznych (np. Scikit-learn, TensorFlow/PyTorch) do analizy danych procesowych i szeregów czasowych.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
[K6_U07] potrafi wykorzystać metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów	Potrafi dobrać odpowiednią metodę detekcji anomalii do charakterystyki danych i specyfiki problemu (np. dane statyczne vs. szereg czasowy), a następnie zinterpretować uzyskane wyniki w celu wsparcia procesu decyzyjnego (np. identyfikacji awarii).	[SU1] Ocena realizacji zadania [SU4] Ocena umiejętności korzystania z metod i narzędzi

Treści przedmiotu

Treści przedmiotu - wykład

1. Wprowadzenie do detekcji anomalii: Definicja anomalii, znaczenie w przemyśle 4.0, medycynie i cyberbezpieczeństwie. Charakterystyka danych procesowych i szeregów czasowych. Klasyfikacja anomalii: punktowe, kontekstowe, zbiorowe.

2. Metody statystyczne: Modele parametryczne (testy hipotez, rozkład Gaussa) i nieparametryczne (histogramy, Kernel Density Estimation). Detekcja oparta na progowaniu statycznym i dynamicznym.

3. Analiza szeregów czasowych i modele predykcyjne: Dekompozycja sygnału (trend, sezonowość). Wykorzystanie modeli regresyjnych (np. ARIMA) do predykcji i wykrywania odchyleń od prognozy.

4. Nienadzorowane uczenie maszynowe: Algorytmy oparte na gęstości (DBSCAN, LOF) i klastrowaniu (k-średnich). Metody oparte na izolacji (Isolation Forest). Zastosowanie autoenkoderów do rekonstrukcji sygnału i detekcji anomalii.

5. Głębokie uczenie w analizie sekwencji: Architektury sieci rekurencyjnych (RNN, LSTM, GRU) do modelowania procesów dynamicznych. Wykorzystanie sieci typu Transformer do analizy długich zależności w danych.

6. Zaawansowane techniki i zastosowania: Wykorzystanie sieci GAN do generowania danych normalnych i wykrywania anomalii. Aplikacje w monitoringu procesów przemysłowych (predictive maintenance), analizie sygnałów EKG/EEG, systemach IoT i cyberbezpieczeństwie. Podsumowanie i trendy rozwojowe.

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Kolokwium pisemne	50.0%	50.0%
Ocena z laboratorium	50.0%	50.0%

<table>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>1. Aggarwal C. C., Outlier Analysis, Springer, 2nd ed., 2017.

2. Chandola V., Banerjee A., Kumar V., Anomaly detection: A survey, ACM computing surveys, 2009.

3. McKinney W., Python for Data Analysis, O'Reilly Media, 2nd ed., 2017.

4. Dokumentacja bibliotek: Scikit-learn, TensorFlow, PyTorch.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. Goodfellow I., Bengio Y., Courville A., Deep Learning, MIT Press, 2016.

2. Hyndman R.J., Athanasopoulos G., Forecasting: principles and practice, OTexts, 3rd ed., 2021.

3. Artykuły naukowe z konferencji (np. NeurIPS, ICML) i czasopism (np. IEEE Transactions) dotyczące detekcji anomalii.</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2">Przykładowe pytania teoretyczne:

1. Proszę zdefiniować i podać przykłady anomalii punktowej, kontekstowej i zbiorowej w kontekście danych z procesów przemysłowych.

2. Wyjaśnij, w jaki sposób autoenkoder może być wykorzystany do wykrywania anomalii. Co jest miarą anomalii w tym podejściu i jak wyznaczyć próg decyzyjny?

3. Porównaj algorytm k-średnich (k-means) i DBSCAN pod kątem ich przydatności w detekcji anomalii. W jakich scenariuszach jeden z nich będzie miał przewagę nad drugim?

4. Opisz, na czym polega wykorzystanie sieci rekurencyjnych (np. LSTM) do wykrywania anomalii w szeregach czasowych. Jakie są zalety tego podejścia w porównaniu do metod statystycznych?

Przykładowe zadania realizowane na laboratorium:

1. Zaimplementuj w języku Python algorytm detekcji anomalii oparty na metodzie ruchomej średniej i odchylenia standardowego (reguła 3-sigma). Przetestuj go na dostarczonym szeregu czasowym i zwizualizuj wykryte anomalie.

2. Wykorzystaj bibliotekę Scikit-learn do zastosowania algorytmu Isolation Forest na zbiorze danych o transakcjach finansowych w celu wykrycia potencjalnych oszustw. Oceń skuteczność modelu.

3. Zbuduj i wytrenuj prosty autoenkoder w bibliotece TensorFlow/Keras na zbiorze danych "normalnych" (np. symulowane dane z czujnika). Następnie wykorzystaj błąd rekonstrukcji do identyfikacji anomalii w zbiorze testowym zawierającym nietypowe próbki.</td></tr>
<tr><td>Zajęcia praktyczne w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.