

KARTA KURSU
realizowanego na specjalności

CYBERBEZPIECZEŃSTWO

Nazwa	Wykrywanie anomalii systemowych z wykorzystaniem metod sztucznej inteligencji
Nazwa w j. ang.	Detecting system anomalies using artificial intelligence methods

Koordinator	Dr.hab., prof. UKEN Serhii Semenov	Zespół dydaktyczny
		Dr.hab., prof. UKEN Serhii Semenov
Punkcja ECTS*	st. stacjonarne: 4 st. niestacjonarne: 4	

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z teoretycznymi podstawami oraz praktycznymi metodami wykrywania anomalii systemowych z wykorzystaniem nowoczesnych technik sztucznej inteligencji. Studenci zdobędą wiedzę na temat klasycznych i zaawansowanych metod detekcji anomalii, nauczą się stosować algorytmy uczenia maszynowego i głębokiego uczenia do analizy danych rzeczywistych, w tym szeregów czasowych, danych sieciowych i danych IoT.

Warunki wstępne

Wiedza	Student powinien posiadać podstawową wiedzę z zakresu: struktur danych i algorytmów, statystyki i rachunku prawdopodobieństwa, podstaw uczenia maszynowego, systemów operacyjnych i sieci komputerowych, języka programowania Python lub innego języka wysokiego poziomu.
Umiejętności	Student powinien potrafić: programować w języku Python (lub innym języku wysokiego poziomu), analizować dane z wykorzystaniem podstawowych narzędzi i bibliotek (np. pandas, numpy), posługiwać się środowiskiem programistycznym i systemem kontroli wersji, implementować i testować proste algorytmy, korzystać z literatury technicznej i dokumentacji w języku angielskim.
Kursy	Zalecane jest wcześniejsze zaliczenie kursów z zakresu: podstaw programowania, algorytmów i struktur danych, podstaw sztucznej inteligencji lub uczenia maszynowego.

Efekty uczenia się

Wiedza	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: W01:	SC_W05
Umiejętności	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: U01:	SC_U06, SC_U08

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: K01:	SC_K01

Studia stacjonarne

Organizacja										
Forma zajęć	Wykład (W)	Ćwiczenia w grupach								
		A		K		L		S		P
Liczba godzin	10					30				

Studia niestacjonarne

Organizacja										
Forma zajęć	Wykład (W)	Ćwiczenia w grupach								
		A		K		L		S		P
Liczba godzin	10					20				

Opis metod prowadzenia zajęć

Zajęcia prowadzone są w formie wykładów oraz laboratoriów, z wykorzystaniem aktywizujących metod kształcenia. Wykłady mają charakter problemowy i prezentacyjny – wprowadzają podstawowe pojęcia, klasyfikacje i techniki wykrywania anomalii, ze szczególnym uwzględnieniem zastosowań w cyberbezpieczeństwie. Część materiału może być udostępniana w formie prezentacji lub materiałów e-learningowych. Laboratoria prowadzone są w trybie praktycznym, zorientowanym na rozwiązywanie rzeczywistych problemów. Studenci pracują indywidualnie lub w małych zespołach, wykorzystując narzędzia programistyczne i środowiska analityczne (np. Python, scikit-learn, pandas, Jupyter Notebook). Zajęcia nastawione są na samodzielną analizę danych, implementację modeli detekcji anomalii oraz interpretację wyników.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Zadania problemowe
W01					X			X					
W02					X			X					
W03					X			X					
U01					X			X					
U02					X			X					
U03					X			X					
K01					X			X					
K02					X			X					
K03					X			X					

Kryteria oceny	<p>Warunkiem zaliczenia kursu jest:</p> <ul style="list-style-type: none"> • uzyskanie pozytywnych ocen z zajęć laboratoryjnych (zaliczenie wszystkich obowiązkowych ćwiczeń), • zaliczenie testu końcowego obejmującego materiał z wykładów. <p>Składniki oceny końcowej:</p> <ul style="list-style-type: none"> • aktywność i wykonanie zadań laboratoryjnych – 60% Ocena obejmuje poprawność i kompletność realizowanych ćwiczeń, samodzielność oraz terminowość. • test końcowy z części teoretycznej (materiał wykładowy) – 40% Pisemny test sprawdzający wiedzę z zakresu pojęć, metod oraz interpretacji wyników. <p>Skala ocen:</p> <ul style="list-style-type: none"> • < 50% – niedostateczny (2,0) • 50–59% – dostateczny (3,0) • 60–69% – dostateczny plus (3,5) • 70–79% – dobry (4,0) • 80–89% – dobry plus (4,5) • 90–100% – bardzo dobry (5,0)
----------------	---

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<ol style="list-style-type: none"> 1. Wprowadzenie do wykrywania anomalii – definicje, typy (punktowe, kontekstowe, kolektywne), zastosowania praktyczne. 2. Systemy wykrywające anomalie – wyjaśnialność modeli, metryki skuteczności (precision, recall, F1-score), ocena porównawcza metod. 3. Tradycyjne podejścia do detekcji anomalii – metody statystyczne, progowe, regresja liniowa. 4. Wstępna analiza danych i eksploracja anomalii. 5. Klasteryzacja i wykrywanie anomalii z użyciem k-NN i DBSCAN. 6. Metody gęstościowe: Local Outlier Factor (LOF). 7. Isolation Forest – teoria i praktyczne zastosowanie. 8. Redukcja wymiarowości i detekcja anomalii za pomocą PCA. 9. Identyfikacja anomalii przy użyciu K-means. 10. Uczenie maszynowe w detekcji anomalii – nadzorowane i nienadzorowane podejścia. 11. Głębokie uczenie: autoenkodery w wykrywaniu anomalii. 12. Wykrywanie anomalii w szeregach czasowych – podejścia klasyczne. 13. Sieci neuronowe LSTM i GRU w analizie danych sekwencyjnych. 14. Detekcja anomalii w danych sieciowych i logach systemowych. 15. Anomalie w danych IoT – przygotowanie, analiza, przykłady.
--

Wykaz literatury podstawowej

<ol style="list-style-type: none"> 1. Emmanuel Tsukerman Machine Learning for Cybersecurity Cookbook. Over 80 recipes on how to implement machine learning algorithms for building security systems using Python Wydawnictwo: Packt Publishing 346 c. 2. Moskalenko, V.; Kharchenko, V.; Semenov, S. Model and Method for Providing Resilience to Resource-Constrained AI-System. Sensors 2024, 24, 5951. https://doi.org/10.3390/s24185951 3. Meleshko, Yelyzaveta V., Mykola Yakymenko and Serhii Semenov. "A Method of Detecting Bot Networks Based on Graph Clustering in the Recommendation System of Social Network." International Conference on Computational Linguistics and Intelligent Systems (2021)

Wykaz literatury uzupełniającej

<ol style="list-style-type: none"> 1. R. Patelski and D. Pazderski, "Parameter Identifying Disturbance Rejection Control With Asymptotic Error Convergence," in IEEE Robotics and Automation Letters, vol. 9, no. 2, pp. 1035-1042, Feb. 2024, doi: 10.1109/LRA.2023.3339942.
--

2. Andreas Fried, Maximilian Stemmer-Grabow, and Julian Wachter. 2023. Register Allocation for Compressed ISAs in LLVM. In Proceedings of the 32nd ACM SIGPLAN International Conference on Compiler Construction (CC 2023). Association for Computing Machinery, New York, NY, USA, 122–132. <https://doi.org/10.1145/3578360.3580261>
3. Schummer, P.; del Rio, A.; Serrano, J.; Jimenez, D.; Sánchez, G.; Llorente, Á. Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation. AI 2024, 5, 2967-2983. <https://doi.org/10.3390/ai5040143>

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia stacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	10
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	10
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	15
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	15
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4