

KARTA KURSU (realizowanego w module specjalności)**Cyberbezpieczeństwo***(nazwa specjalności)*

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

Koordinator	dr hab. Serhii Semenov	Zespół dydaktyczny
		mgr inż. Michał Niemczyk
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

Celem przedmiotu jest zdobycie wiedzy oraz umiejętności praktycznych w zakresie identyfikacji, analizy i wykrywania anomalii występujących w systemach informatycznych przy użyciu metod sztucznej inteligencji (AI). Studenci poznają podstawowe techniki uczenia maszynowego, uczenia głębokiego oraz metod statystycznych stosowanych do wykrywania odstępstw od normalnego działania systemów. Ważnym elementem przedmiotu jest praktyczne zastosowanie narzędzi oraz bibliotek AI do analizy rzeczywistych zbiorów danych, interpretacja wyników oraz projektowanie skutecznych mechanizmów reagowania na wykryte anomalie. Po ukończeniu zajęć studenci będą potrafili samodzielnie dobierać, implementować oraz oceniać metody AI w kontekście zapewnienia bezpieczeństwa i niezawodności systemów informatycznych.

Warunki wstępne

Wiedza	<ul style="list-style-type: none">• Podstawowa wiedza z zakresu uczenia maszynowego oraz algorytmów sztucznej inteligencji.• Znajomość zasad działania systemów informatycznych oraz bezpieczeństwa systemowego.• Podstawowa znajomość metod statystycznych i analizy danych.
Umiejętności	<ul style="list-style-type: none">• Umiejętność programowania w języku Python.• Umiejętność analizy danych oraz stosowania podstawowych bibliotek do uczenia maszynowego (np. TensorFlow, scikit-learn).• Zdolność logicznego rozwiązywania problemów oraz interpretacji wyników eksperymentów.
Kursy	<ul style="list-style-type: none">• Podstawy sztucznej inteligencji lub uczenia maszynowego.• Bezpieczeństwo systemów informatycznych lub bezpieczeństwo sieciowe.• Statystyka lub metody analizy danych.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Wiedza	W01: Zna zaawansowane metody uczenia maszynowego stosowane w wykrywaniu anomalii systemowych;	SC_W05
	W02: Posiada wiedzę na temat technik analizy i oceny wyników uzyskanych z modeli sztucznej inteligencji;	SC_W04
	W03: Rozumie specyfikę zastosowania różnych algorytmów AI w kontekście cyberbezpieczeństwa;	SC_W04 SC_W05
	W04: Zna zasady projektowania i implementacji systemów wykrywających anomalie z wykorzystaniem AI.	SC_W04 SC_W05
	Efekt uczenia się dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Umiejętności	Po zakończeniu kursu student:	
	U01: Potrafi dobrać odpowiednie techniki AI do rozwiązania konkretnego problemu wykrywania anomalii systemowych	SC_U06
	U02: Umie samodzielnie opracować oraz wdrożyć modele wykrywające anomalie na podstawie danych rzeczywistych	SC_U06
	U03: Efektywnie analizuje i interpretuje wyniki działania systemów opartych o uczenie maszynowe oraz potrafi krytycznie ocenić skuteczność stosowanych metod i zaproponować ich udoskonalenie.	SC_U05 SC_U06
	Efekt uczenia się dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Kompetencje społeczne	Po zakończeniu kursu student:	
	K01: Potrafi współpracować w grupie, realizując projekty związane z wykrywaniem anomalii systemowych	SC_K01, SC_K02 , SC_K03
	K02: Wykazuje świadomość znaczenia ciągłego doskonalenia umiejętności w dynamicznie rozwijającej się dziedzinie AI	
	K03: Jest odpowiedzialny za rzetelność analiz danych oraz dokładność przedstawianych wyników	
	K04: Rozumie społeczne konsekwencje stosowania metod AI w bezpieczeństwie informatycznym oraz zachowuje zasady etyki zawodowej	

Studia stacjonarne

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

Studia niestacjonarne

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

Opis metod prowadzenia zajęć

Zajęcia realizowane są w formie łączącej wiedzę teoretyczną z praktycznym podejściem projektowym. Metody prowadzenia zajęć obejmują:

- Wykład interaktywny – przedstawienie podstaw teoretycznych metod wykrywania anomalii z wykorzystaniem sztucznej inteligencji z aktywnym udziałem studentów (zadawanie pytań, dyskusja problemowa).
- Laboratorium komputerowe – samodzielna i zespołowa realizacja praktycznych projektów polegających na analizie rzeczywistych zbiorów danych oraz implementacji modeli AI.
- Analiza przypadków (studia przypadków) – omawianie przykładów zastosowań AI w obszarze bezpieczeństwa systemowego, analiza skuteczności zastosowanych rozwiązań i sposobów ich doskonalenia.
- Ćwiczenia indywidualne z wykorzystaniem SI – realizacja zadań indywidualnych mających na celu praktyczne zastosowanie technik sztucznej inteligencji do wykrywania anomalii systemowych, w tym samodzielne projektowanie, implementacja i ocena modeli AI.

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	Inne
W01					X							X	
W02					X							X	
W03					X							X	
W04					X							X	
U01					X							X	
U02					X							X	
U03					X							X	
K01					X							X	
K02					X							X	
K03					X							X	

Kryteria oceny

Jakość wykonania ćwiczeń indywidualnych: poprawność implementacji, skuteczność zastosowanych modeli SI, interpretacja wyników.

	Terminowość realizacji zadań: oddawanie prac w wyznaczonych terminach. 0-49 punktów – ndst 50-59 punktów – dst 60-69 punktów – dst plus 70-79 punktów – db 80-89 punktów – db plus 90-100 punktów – bdb
--	---

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<ol style="list-style-type: none"> 1. Wprowadzenie do wykrywania anomalii systemowych 2. Klasyczne metody wykrywania anomalii 3. Wykorzystanie nadzorowanego uczenia maszynowego w wykrywaniu anomalii 4. Metody nienadzorowanego uczenia maszynowego 5. Głębokie uczenie w analizie danych sekwencyjnych 6. Generatywne sieci przeciwstawne (GANs) w wykrywaniu anomalii 7. Zastosowanie uczenia ze wzmacnieniem w detekcji anomalii 8. Hybrydowe podejścia w wykrywaniu anomalii 9. Praktyczne narzędzia i platformy wykrywania anomalii 10. Wyzwania praktyczne oraz zalecenia przy wdrażaniu systemów wykrywania anomalii

Wykaz literatury podstawowej (wybrane fragmenty)

<ol style="list-style-type: none"> 1. Systemy wykrywania intruzów wykorzystujące metody sztucznej inteligencji, Marcin Luckner, Marek Szmit, https://www.ippt.pan.pl/Repository/o324.pdf 2. A Survey on Anomaly Detection for Technical Systems using LSTM Networks, Oliver Niggemann, Alexander Maier, Alexander Freytag, https://arxiv.org/abs/2105.13810 3. AI – sztuczna inteligencja w finansach przedsiębiorstw, Katarzyna Prędkiewicz, Krzysztof Biegun, https://www.wir.ue.wroc.pl/docstore/download/UEWR22f5c5aeb10841a9af0d3491e1bb552e/Predki_ewicz_Biegun_AI-sztuczna_inteligencja_w_finansach.pdf 4. Sztuczna inteligencja (AI) jako megatrend kształtujący edukację, Michał Nowakowski, Monika Dawid-Sawicka, Natalia Pawlak, ISBN: 978-83-67100-10-9,
--

Wykaz literatury uzupełniającej

<ol style="list-style-type: none"> 1. Anomaly Detection Principles and Algorithms, Kishan G. Mehrotra, Chilukuri K. Mohan, HuaMing Huang, ISBN: 978-3-319-67524-4 2. Machine Learning and Security: Protecting Systems with Data and Algorithms, Clarence Chio, David Freeman, ISBN: 978-1-4919-7448-4 3. Pattern Recognition and Machine Learning, Christopher M. Bishop ISBN: 978-0387310732

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

Ilość godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć (także w formie nagrań wideo)	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		
Ilość punktów ECTS w zależności od przyjętego przelicznika		75

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

Ilość godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć (także w formie nagrań wideo)	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		
Ilość punktów ECTS w zależności od przyjętego przelicznika		75