Politechnika Krakowska
im. Tadeusza Kościuszki

Program studiów

Wydział:	Wydział Inżynierii Elektrycznej i Komputerowej
Kierunek:	Informatyka i cyberbezpieczeństwo
Poziom studiów:	II stopnia (magister inżynier)
Forma studiów:	studia stacjonarne
Rok akademicki:	2026/27

Spis treści

Charakterystyka kierunku

Informacje podstawowe

Nazwa wydziału:	Wydział Inżynierii Elektrycznej i Komputerowej
Nazwa kierunku:	Informatyka i cyberbezpieczeństwo
Poziom:	II stopnia (magister inżynier)
Profil:	ogólnoakademicki
Forma:	studia stacjonarne
Język studiów:	polski
Klasyfikacja ISCED:	0688

Dziedzina/-y nauki, do której/-ych przyporządkowany jest kierunek studiów

Dziedzina nauk inżynieryjno-technicznych

Przyporządkowanie kierunku do dyscyplin, do których odnoszą się efekty uczenia się

Automatyka, elektronika, elektrotechnika i technologie kosmiczne	60%
Informatyka techniczna i telekomunikacja	40%

Charakterystyka kierunku

Absolwent studiów drugiego stopnia o profilu ogólnoakademickim na kierunku **Informatyka i cyberbezpieczeństwo** uzyskuje tytuł magistra inżyniera. Posiada zaawansowaną wiedzę z zakresu informatyki, cyberbezpieczeństwa oraz nowoczesnych technologii cyfrowych, obejmującą m.in. projektowanie, rozwój i zabezpieczanie systemów informatycznych, analizę i monitorowanie zagrożeń w cyberprzestrzeni, bezpieczeństwo sieci komputerowych, aplikacji i systemów rozproszonych, technologie DevSecOps, ochronę infrastruktury krytycznej, bezpieczeństwo Internetu Rzeczy oraz wykorzystanie metod sztucznej inteligencji w systemach informatycznych i cyberbezpieczeństwie.
Absolwent jest przygotowany do projektowania, wdrażania, integrowania i utrzymania bezpiecznych systemów informatycznych oraz usług cyfrowych. Potrafi analizować zagrożenia, identyfikować podatności, stosować metody ochrony danych i zasobów cyfrowych, a także integrować zagadnienia informatyczne, teleinformatyczne i bezpieczeństwa informacji przy rozwiązywaniu złożonych problemów inżynierskich. Posiada również umiejętność pozyskiwania i krytycznej analizy informacji, opracowywania dokumentacji technicznej oraz pracy projektowej i badawczo-rozwojowej.
Zdobyte kwalifikacje umożliwiają podjęcie pracy w krajowych i międzynarodowych przedsiębiorstwach sektora IT i cyberbezpieczeństwa, firmach teleinformatycznych i przemysłowych, centrach danych, zespołach bezpieczeństwa, instytucjach odpowiedzialnych za ochronę infrastruktury krytycznej, administracji publicznej oraz jednostkach badawczo-rozwojowych. Ukończenie studiów stwarza również możliwość dalszego rozwoju naukowego w szkole doktorskiej.

Efekty uczenia się zostały ustalone uchwałą Senatu PK nr 28 z 22 kwietnia 2026 r. w sprawie ustalenia efektów uczenia się dla studiów II stopnia na kierunku informatyka i cyberbezpieczeństwo prowadzonych przez Wydział Inżynierii Elektrycznej i Komputerowej Politechniki Krakowskiej (https://bip.malopolska.pl/pk,a,2859538,uchwala-nr-28-z-22-kwietnia-2026-r-w-sprawie-ustalenia-efektow-uczenia-sie-dla-studiow-ii-stopnia-na.html).

Efekty uczenia się

Wiedza

Absolwent zna i rozumie

Kod	Treść
EC2-W1	architekturę oraz zasady działania zaawansowanych systemów informatycznych, w tym systemów rozproszonych, czasu rzeczywistego i wieloprocesorowych
EC2-W10	aktualne trendy rozwoju systemów inteligentnych, wizji komputerowej oraz baz danych, w tym grafowych, wraz z ich znaczeniem dla bezpieczeństwa systemów informatycznych
EC2-W11	zasady tworzenia, wdrażania i egzekwowania polityk bezpieczeństwa informacji oraz standardów i regulacji w obszarze cyberbezpieczeństwa
EC2-W12	społeczne, prawne i etyczne uwarunkowania projektowania oraz eksploatacji systemów informatycznych i cyberbezpieczeństwa
EC2-W2	zaawansowane metody i techniki cyberbezpieczeństwa stosowane w ochronie aplikacji, sieci, baz danych, systemów IoT oraz infrastruktury krytycznej
EC2-W3	podstawy teoretyczne oraz praktyczne aspekty kryptografii i protokołów bezpieczeństwa
EC2-W4	metody analizy niezawodności, odporności i ciągłości działania systemów informatycznych oraz zasady zarządzania ryzykiem
EC2-W5	metody sztucznej inteligencji, uczenia maszynowego i analizy danych oraz ich zastosowania w cyberbezpieczeństwie i systemach sieciowych
EC2-W6	nowoczesne paradygmaty programowania, w tym programowanie defensywne, programowanie systemów bezpiecznych oraz robotów przemysłowych
EC2-W7	metody modelowania, analizy i optymalizacji procesów biznesowych oraz systemów informatycznych je wspierających
EC2-W8	architekturę, zasady działania oraz mechanizmy zabezpieczania nowoczesnych sieci komputerowych
EC2-W9	formalne podstawy informatyki kwantowej, w szczególności model obliczeń kwantowych oraz zasady działania i ograniczenia współczesnych systemów i algorytmów kwantowych, w tym ich znaczenie dla bezpieczeństwa

Umiejętności

Absolwent potrafi

Kod	Treść
EC2-U1	pozyskiwać informacje z literatury, baz danych i innych źródeł, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie
EC2-U10	krytycznie analizować i integrować nowoczesne technologie informatyczne, w tym elementy informatyki kwantowej, w celu rozwiązywania złożonych problemów technicznych
EC2-U11	opracowywać i wdrażać polityki bezpieczeństwa informacji oraz procedury zarządzania ryzykiem w organizacjach oraz oceniać i projektować rozwiązania informatyczne z uwzględnieniem aspektów społecznych, prawnych i etycznych

Kod	Treść
EC2-U12	posługiwać się językiem obcym na poziomie co najmniej B2+ Europejskiego Systemu Opisu Kształcenia Językowego, w tym brać udział w dyskusji, oraz prezentować treści z użyciem specjalistycznej terminologii z zakresu kierunku studiów
EC2-U13	kierując się normami etycznymi, podejmować decyzje uwzględniając ich oddziaływanie społeczne i środowiskowe
EC2-U14	porozumiewać się w sposób precyzyjny i spójny prowadząc efektywną komunikację, mediacje i negocjacje
EC2-U2	integrować wiedzę z dziedziny elektrotechniki, automatyki, informatyki, elektroniki i innych dyscyplin, stosując podejście systemowe
EC2-U3	projektować, implementować i analizować złożone systemy informatyczne z uwzględnieniem wymagań bezpieczeństwa, niezawodności i wydajności
EC2-U4	identyfikować, analizować i oceniać zagrożenia cyberbezpieczeństwa oraz dobierać i stosować adekwatne środki ochrony
EC2-U5	stosować metody kryptograficzne i protokoły bezpieczeństwa w celu ochrony danych oraz komunikacji w systemach informatycznych
EC2-U6	projektować, implementować i testować bezpieczne aplikacje webowe, mobilne i rozproszone zgodnie z zasadami programowania w tym programowania defensywnego
EC2-U7	wykorzystywać metody sztucznej inteligencji i analizy danych do detekcji, analizy i prognozowania cyberzagrożeń
EC2-U8	konfigurować, monitorować i zabezpieczać zaawansowane sieci komputerowe, systemy IoT oraz systemy czasu rzeczywistego oraz modelować, symulować i analizować procesy biznesowe, złożone systemy informatyczne jak również projektować i wdrażać bezpieczne rozwiązania bazodanowe, w tym grafowe bazy danych
EC2-U9	programować i integrować roboty przemysłowe oraz systemy inteligentne w środowiskach przemysłowych i sieciowych

Kompetencje społeczne

Absolwent jest gotów do

Kod	Treść
EC2-K1	krytycznej oceny własnej wiedzy i umiejętności oraz ciągłego uczenia się w obszarze informatyki i cyberbezpieczeństwa
EC2-K2	odpowiedzialnego pełnienia ról zawodowych związanych z projektowaniem, wdrażaniem i utrzymaniem systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa
EC2-K3	przestrzegania zasad etyki zawodowej oraz odpowiedzialności za skutki społeczne, prawne i środowiskowe stosowanych rozwiązań informatycznych
EC2-K4	działania zgodnie z obowiązującymi regulacjami, normami i politykami bezpieczeństwa informacji w organizacjach krajowych i międzynarodowych
EC2-K5	współpracy w zespołach interdyscyplinarnych i międzynarodowych, w tym do komunikowania się ze specjalistami z innych dziedzin oraz inicjowania i uczestnictwa w projektach badawczych, rozwojowych i innowacyjnych, także w środowisku międzynarodowym

Wskaźniki programu

Nazwa	
Potwierdzenie – na podstawie planu studiów, że student realizuje zajęcia z dziedziny nauk humanistycznych i/lub społecznych, którym przypisano nie mniej niż 5 punktów ECTS	6
Potwierdzenie – na podstawie planu studiów, że student ma możliwość wyboru zajęć, którym łącznie przypisano liczbę punktów ECTS nie niższą niż 30% ECTS określonych dla programu tych studiów.	28/90 (31.11%)
Potwierdzenie, że dla studiów stacjonarnych co najmniej 50% liczby punktów ECTS określonej dla programu tych studiów realizowanych jest w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	49/90 (54.44%)
Potwierdzenie, że program studiów o profilu ogólnoakademickim obejmuje zajęcia związane z prowadzoną w uczelni działalnością naukową, w wymiarze większym niż 50% liczby punktów ECTS, określonej dla programu tych studiów	80/90 (88.89%)
Potwierdzenie, że liczba punktów ECTS uzyskanych w programie studiów poprzez realizację zajęć z wykorzystaniem metod i technik kształcenia na odległość jest nie wyższa niż 75% ogólnej liczby punktów ECTS w programie studiów o profilu ogólnoakademickim	14/90 (15.56%)
LIczba godzin w programie	1162
Liczba punktów ECTS w programie	90

Plan studiów

Semestr 1

Zajęcia	Forma zajęć / liczba godzin	Forma zaliczenia	Punkty ECTS	Obligatoryjność
Język obcy	Ćwiczenia: 15	Zaliczenie	1	Blok przedmiotów wybieralnych
Język angielski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język niemiecki	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język francuski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język rosyjski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Międzynarodowa mobilność i rozwój naukowy	Seminaria: 30	Zaliczenie	2	Obowiązkowy
Modelowanie i zarządzanie procesami biznesowymi	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	3	Obowiązkowy
Niezawodność i odporność systemów wieloprocesorowych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria: 30 Projekty: 15	Zaliczenie	4	Obowiązkowy
Programowanie robotów przemysłowych	Wykłady: 10; w tym zajęcia zdalne: • Wykłady synchroniczne: 10 Laboratoria: 40 Projekty: 10	Zaliczenie	4	Obowiązkowy
Bezpieczeństwo aplikacji webowych i mobilnych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 30	Zaliczenie	4	Obowiązkowy
Kryptografia	Wykłady: 10; w tym zajęcia zdalne: • Wykłady synchroniczne: 10 Laboratoria komputerowe: 30	Egzamin	3	Obowiązkowy

Zajęcia	Forma zajęć / liczba godzin	Forma zaliczenia	Punkty ECTS	Obligatoryjność
Programowanie defensywne	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30 Laboratoria komputerowe: 20 Projekty: 20	Zaliczenie	4	Obowiązkowy
Bezpieczeństwo infrastruktury krytycznej	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria: 45	Egzamin	5	Obowiązkowy
Suma	**440**		**30**	

Semestr 2

Zajęcia	Forma zajęć / liczba godzin	Forma zaliczenia	Punkty ECTS	Obligatoryjność
Język obcy	Ćwiczenia: 15	Zaliczenie	1	Blok przedmiotów wybieralnych
Język angielski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język niemiecki	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język francuski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Język rosyjski	Ćwiczenia: 15	Zaliczenie	1	Wybieralny
Przedmiot wybieralny 1	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30	Zaliczenie	2	Blok przedmiotów wybieralnych
Społeczne aspekty cyberbezpieczeństwa	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30	Zaliczenie	2	Wybieralny
Etyka w cyberbezpieczeństwie	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30	Zaliczenie	2	Wybieralny
Systemy operacyjne czasu rzeczywistego	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria: 15 Projekty: 15	Zaliczenie	2	Obowiązkowy

Zajęcia	Forma zajęć / liczba godzin	Forma zaliczenia	Punkty ECTS	Obligatoryjność
Cyberbezpieczeństwo i analiza danych	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30 Laboratoria komputerowe: 30	Zaliczenie	4	Obowiązkowy
Sztuczna inteligencja w usługach sieciowych	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30 Laboratoria komputerowe: 30	Egzamin	4	Obowiązkowy
Bezpieczeństwo w IoT	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria: 20 Projekty: 20	Zaliczenie	4	Obowiązkowy
Systemy detekcji i analizy cyberzagrożeń	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria: 45	Egzamin	4	Obowiązkowy
Bezpieczeństwo systemów rozproszonych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 30	Zaliczenie	4	Obowiązkowy
Współczesne metody sztucznej inteligencji	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 20 Projekty: 20	Zaliczenie	3	Obowiązkowy
Grafowe bazy danych i ich zastosowania	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Obowiązkowy
Suma	**485**		**30**	

Semestr 3

Zajęcia	Forma zajęć / liczba godzin	Forma zaliczenia	Punkty ECTS	Obligatoryjność
Polityki bezpieczeństwa i zarządzanie ryzykiem	Wykłady: 30; w tym zajęcia zdalne: • Wykłady synchroniczne: 30	Zaliczenie	2	Obowiązkowy
Bezpieczeństwo w bazach danych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Obowiązkowy
Podstawy informatyki kwantowej i programowania systemów kwantowych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Obowiązkowy
Przedmiot wybieralny 2	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Blok przedmiotów wybieralnych
Zaawansowane modelowanie i analiza systemów informatycznych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Wybieralny
Zaawansowane sieci komputerowe	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Laboratoria komputerowe: 15 Projekty: 15	Zaliczenie	2	Wybieralny
Przedmiot wybieralny 3	Suma godzin kontaktowych: 30	Zaliczenie	2	Blok przedmiotów wybieralnych
Wizja komputerowa w systemach inteligentnych	Wykłady: 15; w tym zajęcia zdalne: • Wykłady synchroniczne: 15 Projekty: 15	Zaliczenie	2	Wybieralny
Kształcenie projektowe	Projekty: 30	Zaliczenie	2	Wybieralny
Seminarium dyplomowe	Seminaria: 30	Zaliczenie	2	Obowiązkowy
Przygotowanie pracy dyplomowej	Seminaria: 12	Zaliczenie	18	Obowiązkowy
Suma	**237**		**30**	

O - Obowiązkowy
W - Wybieralny
B - Blok przedmiotów wybieralnych

Matryca pokrycia efektów kierunkowych

2026/27/S/2/WE/EC/all

Przedmiot	Specjalność	Obligatoryjność	Semestr	EC2-W1	EC2-W10	EC2-W11	EC2-W12	EC2-W2	EC2-W3	EC2-W4	EC2-W5	EC2-W6	EC2-W7	EC2-W8	EC2-W9	EC2-U1	EC2-U10	EC2-U11	EC2-U12	EC2-U13	EC2-U14	EC2-U2	EC2-U3	EC2-U4	EC2-U5	EC2-U6	EC2-U7	EC2-U8	EC2-U9	EC2-K1	EC2-K2	EC2-K3	EC2-K4	EC2-K5
Język angielski		W	1s i 2s																x															
Język niemiecki		W	1s i 2s																x															
Język francuski		W	1s i 2s																x															
Język rosyjski		W	1s i 2s																x															
Międzynarodowa mobilność i rozwój naukowy		O	1s				x									x	x		x															x
Modelowanie i zarządzanie procesami biznesowymi		O	1s				x						x									x						x						x
Niezawodność i odporność systemów wieloprocesorowych		O	1s	x						x													x	x							x			
Programowanie robotów przemysłowych		O	1s									x											x						x		x			
Bezpieczeństwo aplikacji webowych i mobilnych		O	1s					x				x											x	x		x						x		

Przedmiot	Specjalność	Obligatoryjność	Semestr	EC2-W1	EC2-W10	EC2-W11	EC2-W12	EC2-W2	EC2-W3	EC2-W4	EC2-W5	EC2-W6	EC2-W7	EC2-W8	EC2-W9	EC2-U1	EC2-U10	EC2-U11	EC2-U12	EC2-U13	EC2-U14	EC2-U2	EC2-U3	EC2-U4	EC2-U5	EC2-U6	EC2-U7	EC2-U8	EC2-U9	EC2-K1	EC2-K2	EC2-K3	EC2-K4	EC2-K5
Kryptografia		O	1s						x																x						x			
Programowanie defensywne		O	1s									x														x					x			
Bezpieczeństwo infrastruktury krytycznej		O	1s			x		x		x								x			x			x						x		x	
Społeczne aspekty cyberbezpieczeństwa		W	2s		x		x													x											x		x
Etyka w cyberbezpieczeństwie		W	2s			x	x											x		x											x		
Systemy operacyjne czasu rzeczywistego		O	2s	x																		x					x			x			
Cyberbezpieczeństwo i analiza danych		O	2s								x					x					x						x			x	x			
Sztuczna inteligencja w usługach sieciowych		O	2s								x			x			x										x			x				
Bezpieczeństwo w IoT		O	2s					x						x										x				x				x		
Systemy detekcji i analizy cyberzagrożeń		O	2s								x													x				x						
Bezpieczeństwo systemów rozproszonych		O	2s	x				x															x	x									x	
Współczesne metody sztucznej inteligencji		O	2s								x										x						x					x		
Grafowe bazy danych i ich zastosowania		O	2s		x																							x		x				

Przedmiot	Specjalność	Obligatoryjność	Semestr	EC2-W1	EC2-W10	EC2-W11	EC2-W12	EC2-W2	EC2-W3	EC2-W4	EC2-W5	EC2-W6	EC2-W7	EC2-W8	EC2-W9	EC2-U1	EC2-U10	EC2-U11	EC2-U12	EC2-U13	EC2-U14	EC2-U2	EC2-U3	EC2-U4	EC2-U5	EC2-U6	EC2-U7	EC2-U8	EC2-U9	EC2-K1	EC2-K2	EC2-K3	EC2-K4	EC2-K5
Polityki bezpieczeństwa i zarządzanie ryzykiem		O	3s			x				x								x			x			x								x	
Bezpieczeństwo w bazach danych		O	3s					x																	x			x			x			
Podstawy informatyki kwantowej i programowania systemów kwantowych		O	3s												x		x													x				
Zaawansowane modelowanie i analiza systemów informatycznych		W	3s	x									x									x	x							x				
Zaawansowane sieci komputerowe		W	3s											x														x			x			
Wizja komputerowa w systemach inteligentnych		W	3s		x																					x		x		x				
Kształcenie projektowe		W	3s			x											x					x	x							x	x			x
Seminarium dyplomowe		O	3s			x	x									x				x	x									x				x
Przygotowanie pracy dyplomowej		O	3s			x	x									x				x	x									x				x
Suma (obowiązkowy):				3	1	4	4	5	1	3	4	3	1	2	1	4	3	2	1	2	6	1	5	7	2	2	4	5	1	7	8	3	3	4
Suma (wybieralny):				1	2	2	2	0	0	0	0	0	1	1	0	0	1	1	4	2	0	2	2	0	0	0	1	1	1	3	2	2	0	2
Suma:				4	3	6	6	5	1	3	4	3	2	3	1	4	4	3	5	4	6	3	7	7	2	2	5	6	2	10	10	5	3	6

Politechnika Krakowska
im. Tadeusza Kościuszki

Język angielski

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.23.00741.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty ogólne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Cele kształcenia dla zajęć

Kod	Cel
C1	Rozwijanie zdolności skutecznego komunikowania się studentów w języku obcym w typowych sytuacjach akademickich i zawodowych, z uwzględnieniem specyfiki studiowanego kierunku, w tym udziału w dyskusjach na tematy związane z kierunkiem studiów.
C2	Przygotowanie studentów do rozumienia oraz tworzenia wypowiedzi ustnych i/lub pisemnych w języku obcym, opartych na treściach kierunkowych i z wykorzystaniem podstawowej terminologii specjalistycznej.
C3	Kształtowanie umiejętności selekcji, interpretacji oraz funkcjonalnego przetwarzania informacji pochodzących z obcojęzycznych tekstów źródłowych, zarówno pisanych, jak i mówionych.
C4	Rozwijanie umiejętności współpracy i komunikacji w zespole w wielokulturowym środowisku akademickim.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Umiejętności – Student/ka:			
U1	rozumie ogólny sens oraz istotne informacje zawarte w obcojęzycznych tekstach pisanych i mówionych o charakterze kierunkowym.	EC2-U12	Odpowiedź ustna, Projekt, Test, Zaliczenie pisemne, Obserwacja pracy studenta
U2	formułuje spójne, zrozumiałe i adekwatne do sytuacji wypowiedzi ustne w języku obcym, z wykorzystaniem terminologii właściwej dla studiowanego kierunku.	EC2-U12	Odpowiedź ustna, Prezentacja, Projekt, Zaliczenie ustne
U3	tworzy krótkie wypowiedzi pisemne w języku obcym (np. opis, streszczenie, e-mail formalny, prezentacja treści technicznych), zachowując poprawność komunikacyjną i językową.	EC2-U12	Projekt, Test, Zaliczenie pisemne
U4	selekcjonuje i krytycznie przetwarza informacje pochodzące z obcojęzycznych źródeł, prezentując je w formie ustnej i/lub pisemnej.	EC2-U12	Odpowiedź ustna, Prezentacja, Projekt, Test, Zaliczenie pisemne, Zaliczenie ustne, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Słownictwo związane z podstawami cyberbezpieczeństwa i krajobrazem zagrożeń, kryptografią i ochroną danych.	U1, U2, U3, U4	Ćwiczenia
2.	Terminologia dotycząca bezpieczeństwa sieci i aplikacji, analizy incydentów i forensics.	U1, U2, U3, U4	Ćwiczenia
3.	Słownictwo związane z bezpieczeństwem chmur i nowoczesnych technologii – cloud security (AWS/Azure), containter security, zero-trust, IoT/OT.	U1, U2, U3, U4	Ćwiczenia

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Zagadnienia leksykalne dotyczące komunikacji zawodowej i compliance – raporty techniczne, prezentacje, standardy (NIST, ISO 27001, GDPR)	U1, U2, U3, U4	Ćwiczenia
5.	Słownictwo związane z poszukiwaniem pracy: CV, rozmowa kwalifikacyjna.	U1, U2, U3, U4	Ćwiczenia
6.	Język i struktury stosowane w prezentacjach technicznych oraz techniki prowadzenia prezentacji.	U1, U2, U4	Ćwiczenia

Nakład pracy studenta i punkty ECTS

Semestr 1

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	2
Przygotowanie się do kolokwiów i egzaminów	2
Przygotowanie sprawozdań, raportów, projektów, prezentacji	2
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Semestr 2

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	2
Przygotowanie się do kolokwiów i egzaminów	2

Przygotowanie sprawozdań, raportów, projektów, prezentacji	2
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Język niemiecki

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.23.00745.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty ogólne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Cele kształcenia dla zajęć

Kod	Cel
C1	Doskonalenie kompetencji komunikacyjnych studentów w języku obcym w środowisku akademickim i zawodowym, z uwzględnieniem problematyki studiowanego kierunku.
C2	Przygotowanie studentów do aktywnego udziału w dyskusjach merytorycznych oraz prezentowania treści specjalistycznych w języku obcym, z wykorzystaniem terminologii właściwej dla kierunku studiów.
C3	Rozwijanie umiejętności krytycznej analizy, syntezy i interpretacji informacji pochodzących z obcojęzycznych źródeł specjalistycznych.
C4	Kształtowanie autonomii w doskonaleniu kompetencji językowych oraz odpowiedzialnego funkcjonowania w zespołach projektowych i środowisku zawodowym.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Umiejętności – Student/ka:			
U1	określa szczegółowe treści oraz informacje zawarte w złożonych obcojęzycznych tekstach pisanych i mówionych o charakterze specjalistycznym.	EC2-U12	Odpowiedź ustna, Test, Obserwacja pracy studenta
U2	bierze aktywny udział w dyskusjach merytorycznych w języku obcym, formułując spójne argumenty oraz reagując na wypowiedzi innych uczestników.	EC2-U12	Odpowiedź ustna, Obserwacja pracy studenta
U3	przygotowuje i prezentuje w języku obcym treści specjalistyczne związane z kierunkiem studiów, w sposób uporządkowany, precyzyjny i adekwatny do odbiorcy.	EC2-U12	Test, Obserwacja pracy studenta
U4	syntetyzuje i krytycznie przetwarza informacje z obcojęzycznych źródeł specjalistycznych, prezentując wnioski w formie ustnej lub pisemnej.	EC2-U12	Odpowiedź ustna, Test, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawowa terminologia z zakresu informatyki; sprzęt komputerowy i urządzenia peryferyjne; podstawowe zagadnienia związane z eksploatacją sprzętu komputerowego; urządzenia cyfrowe i ich zastosowania.	U1, U2, U4	Ćwiczenia
2.	Podstawowe zagadnienia związane z funkcjonowaniem sieci komputerowych, transmisją danych, usługami sieciowymi, Internetem rzeczy (IoT), technologiami mobilnymi oraz usługami chmurowymi.	U1, U2, U4	Ćwiczenia
3.	Podstawowe pojęcia związane z ochroną informacji, bezpieczeństwem systemów informatycznych, zarządzaniem ryzykiem oraz kulturą cyberbezpieczeństwa.	U1, U2, U3, U4	Ćwiczenia

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Cyfryzacja procesów, automatyzacja, robotyzacja, inteligentne systemy, innowacje i technologie przyszłości.	U1, U2, U3, U4	Ćwiczenia
5.	Język i struktury stosowane w prezentacjach technicznych oraz techniki prowadzenia prezentacji.	U1, U2, U3, U4	Ćwiczenia
6.	Słownictwo związane z poszukiwaniem pracy: CV, rozmowa kwalifikacyjna.	U1, U2, U3, U4	Ćwiczenia

Nakład pracy studenta i punkty ECTS

Semestr 1

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	2
Przygotowanie się do zajęć	3
Przygotowanie się do kolokwiów i egzaminów	3
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Semestr 2

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	2
Przygotowanie się do zajęć	2
Przygotowanie się do kolokwiów i egzaminów	2
Przygotowanie prezentacji multimedialnej	2

Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Język francuski

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.23.00744.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty ogólne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Cele kształcenia dla zajęć

Kod	Cel
C1	Doskonalenie zaawansowanych kompetencji komunikacyjnych studentów w języku obcym w środowisku akademickim i zawodowym, z uwzględnieniem problematyki studiowanego kierunku.
C2	Przygotowanie studentów do aktywnego udziału w dyskusjach merytorycznych oraz prezentowania treści specjalistycznych w języku obcym, z wykorzystaniem terminologii właściwej dla kierunku studiów.
C3	Rozwijanie umiejętności krytycznej analizy, syntezy i interpretacji informacji pochodzących z obcojęzycznych źródeł specjalistycznych.
C4	Kształtowanie autonomii w doskonaleniu kompetencji językowych oraz odpowiedzialnego funkcjonowania w zespołach projektowych i środowisku zawodowym.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Umiejętności – Student/ka:			
U1	rozumie szczegółowe treści oraz implikacje zawarte w złożonych obcojęzycznych tekstach pisanych i mówionych o charakterze specjalistycznym.	EC2-U12	Odpowiedź ustna, Prezentacja, Test, Zaliczenie pisemne, Obserwacja pracy studenta
U2	bierze aktywny udział w dyskusjach merytorycznych w języku obcym, formułując spójne argumenty oraz reagując na wypowiedzi innych uczestników.	EC2-U12	Odpowiedź ustna, Prezentacja, Test, Zaliczenie pisemne, Obserwacja pracy studenta
U3	przygotowuje i prezentuje w języku obcym treści specjalistyczne związane z kierunkiem studiów, w sposób uporządkowany, precyzyjny i adekwatny do odbiorcy.	EC2-U12	Odpowiedź ustna, Prezentacja, Test, Zaliczenie pisemne, Obserwacja pracy studenta
U4	syntetyzuje i krytycznie przetwarza informacje z obcojęzycznych źródeł specjalistycznych, prezentując wnioski w formie ustnej lub pisemnej.	EC2-U12	Odpowiedź ustna, Prezentacja, Test, Zaliczenie pisemne, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Zagadnienia leksykalne związane z funkcjonowaniem w środowisku zawodowym: życiorys , rozmowa kwalifikacyjna, przedstawianie swoich osiągnięć, elementy korespondencji biznesowej (opcjonalnie).	U1, U2, U3, U4	Ćwiczenia

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
2.	Zagadnienia leksykalne związane z różnymi dziedzinami działalności inżynierów : etapy projektowania, techniczny opis projektu, etapy realizacji, narzędzia informatyczne.	U1, U2, U3, U4	Ćwiczenia
3.	Słownictwo i struktury leksykalno-gramatyczne potrzebne w pracy z tekstami specjalistycznymi z dziedziny cyberbezpieczeństwa, infotroniki, informatyki oraz do dyskusji na tematy związane ze specjalnością studiów: bezpieczeństwo w sieci a internet rzeczy (IoT), roboty i sztuczna inteligencja, innowacje technologiczne, , oraz inne tematy zaproponowane przez studentów.	U1, U2, U3, U4	Ćwiczenia
4.	Zagadnienia związane z prezentacją techniczną: narzędzia leksykalno-gramatyczne do opisu projektu (wygląd, działanie), schematów (grafów), zasady prezentacji w języku francuskim.	U1, U2, U3, U4	Ćwiczenia

Nakład pracy studenta i punkty ECTS

Semestr 1

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	1
Przygotowanie sprawozdań, raportów, projektów, prezentacji	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	3
Przygotowanie się do kolokwiów i egzaminów	2
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Semestr 2

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15

Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	1
Przygotowanie prezentacji multimedialnej	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	3
Przygotowanie się do kolokwiów i egzaminów	2
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Język rosyjski

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.23.00747.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty ogólne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Ćwiczenia: 15	1

Cele kształcenia dla zajęć

Kod	Cel
C1	Doskonalenie zaawansowanych kompetencji komunikacyjnych studentów w języku obcym w środowisku akademickim i zawodowym, z uwzględnieniem problematyki studiowanego kierunku.
C2	Przygotowanie studentów do aktywnego udziału w dyskusjach merytorycznych oraz prezentowania treści specjalistycznych w języku obcym, z wykorzystaniem terminologii właściwej dla kierunku studiów.
C3	Rozwijanie umiejętności krytycznej analizy, syntezy i interpretacji informacji pochodzących z obcojęzycznych źródeł specjalistycznych.
C4	Kształtowanie autonomii w doskonaleniu kompetencji językowych oraz odpowiedzialnego funkcjonowania w zespołach projektowych i środowisku zawodowym.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Umiejętności – Student/ka:			
U1	rozumie szczegółowe treści oraz implikacje zawarte w złożonych obcojęzycznych tekstach pisanych i mówionych o charakterze specjalistycznym.	EC2-U12	Odpowiedź ustna, Test, Obserwacja pracy studenta
U2	bierze aktywny udział w dyskusjach merytorycznych w języku obcym, formułując spójne argumenty oraz reagując na wypowiedzi innych uczestników.	EC2-U12	Odpowiedź ustna, Obserwacja pracy studenta
U3	przygotowuje i prezentuje w języku obcym treści specjalistyczne związane z kierunkiem studiów, w sposób uporządkowany, precyzyjny i adekwatny do odbiorcy.	EC2-U12	Odpowiedź ustna, Test, Obserwacja pracy studenta
U4	syntetyzuje i krytycznie przetwarza informacje z obcojęzycznych źródeł specjalistycznych, prezentując wnioski w formie ustnej lub pisemnej.	EC2-U12	Odpowiedź ustna, Test, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Zagadnienia leksykalne związane z wybranym kierunkiem studiów (wybrane zagadnienia): Zagrożenia sieciowe: malware, ransomware, phishing, DDoS. Kryptografia: szyfrowanie symetryczne i asymetryczne, podpisy cyfrowe, infrastruktura klucza publicznego (PKI). Bezpieczeństwo systemów: polityki bezpieczeństwa, testy penetracyjne (pentesting), audyty bezpieczeństwa. Infrastruktura chmurowa i IoT: modele chmurowe (IaaS, PaaS, SaaS), bezpieczeństwo Internetu Rzeczy. Uczenie maszynowe (Machine Learning): sieci neuronowe, uczenie nadzorowane i nienadzorowane. Przetwarzanie danych: eksploracja danych (Data Mining), big data.	U1, U2, U3, U4	Ćwiczenia

Nakład pracy studenta i punkty ECTS

Semestr 1

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Przygotowanie się do zajęć	2
Przygotowanie się do kolokwiów i egzaminów	5
Konsultacje przedmiotowe	1
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Semestr 2

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Ćwiczenia	15
Egzaminy i zaliczenia w sesji	2
Przygotowanie się do zajęć	1
Przygotowanie się do kolokwiów i egzaminów	2
Przygotowanie prezentacji multimedialnej	4
Konsultacje przedmiotowe	1
Łączny nakład pracy studenta	**Liczba godzin** 25
Liczba punktów ECTS	**ECTS** 1

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Międzynarodowa mobilność i rozwój naukowy

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04145.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty humanistyczne i społeczne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Seminaria: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Przygotowanie studentów do funkcjonowania w międzynarodowym środowisku naukowym i przemysłowym oraz rozwijanie kompetencji związanych z komunikacją naukową, mobilnością międzynarodową i planowaniem kariery zawodowej.
C2	Identyfikacja i wspieranie studentów zainteresowanych działalnością badawczą oraz stworzenie warunków do ich dalszego rozwoju naukowego, w tym kontynuacji kształcenia w szkole doktorskiej i zaangażowania w projekty badawczo-rozwojowe realizowane na Wydziale.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	określa możliwości rozwoju naukowego i zawodowego w międzynarodowych ośrodkach akademickich i przemysłowych oraz zasady funkcjonowania projektów badawczo-rozwojowych oraz programów mobilności.	EC2-W12	Projekt
W2	definiuje strukturę artykułu naukowego i zasady etyki publikacyjnej oraz formy prezentacji wyników badań na konferencjach i seminariach.	EC2-W12	Projekt
Umiejętności – Student/ka:			
U1	obsługuje wyszukiwarki międzynarodowych ofert pracy, staży i programów wymiany.	EC2-U1, EC2-U12	Projekt
U2	proponuje i przygotowuje abstrakt i krótki artykuł techniczny w języku angielskim w opraciu o wybrany schemat, np. IEEE Xplore. Wykonuje analizę literatury naukowej z wykorzystaniem baz Scopus i Web of Science, Przygotowuje prezentację konferencyjną i przedstawia wyniki swojej pracy; korzysta z narzędzi wspomagających pracę naukową i zarządzanie bibliografią.	EC2-U1, EC2-U10, EC2-U12	Projekt
Kompetencji społecznych – Student/ka:			
K1	identyfikuje potrzebę i znaczenie współpracy międzynarodowej, w tym współpracy w międzynarodowych zespołach interdyscyplinarnych.	EC2-K5	Projekt
K2	dostrzega potrzebę ciągłego rozwoju zawodowego i naukowego opartego o zasady etyki badań i własności intelektualnej.	EC2-K5	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Ścieżki rozwoju kariery naukowej w kraju i za granicą, w tym programy mobilności międzynarodowej (CEEPUS, Erasmus+, DAAD, NAWA, Marie Curie, EIT, itp.). Wiodące ośrodki naukowe i przemysłowe w dziedzinie informatyki, automatyki, AI i robotyki oraz programy stażowe instytucji badawczych (CERN, ESA, ITER, itp.). Współpraca nauki z przemysłem i projekty B+R. Budowanie tożsamości i związku z uczelnią (np. Rada Przedsiębiorców, Stowarzyszenie Wychowanków, itd.)	W1, U1, K1, K2	Seminaria
2.	Wprowadzenie do komunikacji naukowej, w tym: rola komunikacji naukowej,formy komunikacji naukowej, wyszukiwanie literatury i analiza publikacji, struktura artykułu naukowego i proces recenzji, etyka publikacyjna i wykorzystanie narzędzi AI w pracy naukowej, przygotowanie wystąpień konferencyjnych i posterów, budowanie profilu zawodowego (CV, LinkedIn, ORCID, ResearchGate).	W2, U2, K1, K2	Seminaria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Seminaria	30
Egzaminy i zaliczenia w sesji	2
Przygotowanie sprawozdań, raportów, projektów, prezentacji	18
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Modelowanie i zarządzanie procesami biznesowymi

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04168.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie studentom uporządkowanej wiedzy z zakresu identyfikacji, opisu, modelowania i analizy procesów biznesowych z wykorzystaniem notacji BPMN oraz podstawowych pojęć zarządzania procesowego.
C2	Rozwinięcie umiejętności tworzenia czytelnych modeli procesów biznesowych, obejmujących role, zdarzenia, czynności, bramki decyzyjne, przepływy, komunikację między uczestnikami oraz dokumentowanie reguł i wyjątków procesu.
C3	Kształtowanie umiejętności analizy i usprawniania procesów z wykorzystaniem mierników efektywności, identyfikacji wąskich gardeł, ryzyk, punktów kontrolnych oraz możliwości automatyzacji i cyfryzacji procesu.
C4	Zapoznanie studentów z nowoczesnymi narzędziami i praktykami zarządzania procesami biznesowymi, w tym z systemami workflow/BPMS, podstawami process mining, RPA, podejściem ciągłego doskonalenia oraz współpracą zespołową przy projektowaniu zmian organizacyjnych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Charakteryzuje podejście procesowe w organizacji, podstawowe pojęcia zarządzania procesami biznesowymi oraz zasady modelowania procesów z wykorzystaniem notacji BPMN.	EC2-W12	Test
W2	Opisuje metody analizy, pomiaru i doskonalenia procesów biznesowych, w tym identyfikację interesariuszy, mierników KPI, ryzyk, wąskich gardeł, punktów kontrolnych oraz możliwości automatyzacji procesu.	EC2-W7	Test
W3	Potrafi opracować model procesu biznesowego w notacji BPMN, obejmujący uczestników procesu, zdarzenia, czynności, decyzje, przepływy sterowania i komunikację między rolami.	EC2-W12, EC2-W7	Projekt, Test
Umiejętności – Student/ka:			
U1	Potrafi analizować i usprawniać proces biznesowy, wskazywać problemy organizacyjne i techniczne, proponować warianty zmian oraz przygotować dokumentację procesu i rekomendacje wdrożeniowe.	EC2-U2, EC2-U8	Projekt, Sprawozdanie
U2	Potrafi opracować model procesu biznesowego w notacji BPMN, obejmujący uczestników procesu, zdarzenia, czynności, decyzje, przepływy sterowania i komunikację między rolami.	EC2-U8	Projekt, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	Współpracuje w zespole projektowym, komunikuje się z interesariuszami, krytycznie ocenia przyjęte modele procesów oraz odpowiedzialnie planuje i dokumentuje pracę nad usprawnieniem procesu.	EC2-K5	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do zarządzania procesami biznesowymi: organizacja procesowa, proces, procedura, właściciel procesu, interesariusze, cel i wartość procesu.	W1	Wykłady, Wykłady synchroniczne
2.	Identyfikacja i opis procesu biznesowego: zakres procesu, wejścia i wyjścia, role, odpowiedzialności, reguły biznesowe, dokumenty i przepływ informacji.	W1, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
3.	Notacja BPMN: zdarzenia, aktywności, bramki, przepływy sekwencji i komunikatów, pule, tory, artefakty oraz zasady tworzenia czytelnych diagramów.	W1, W3, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
4.	Modelowanie procesów typu as-is i to-be: dokumentowanie stanu obecnego, analiza problemów, projektowanie wariantu docelowego i uzasadnienie zmian.	W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
5.	Analiza efektywności procesu: mierniki KPI, czasy realizacji, koszty, jakość, SLA, wąskie gardła, punkty decyzyjne i ryzyka operacyjne.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
6.	Analiza efektywności procesu: mierniki KPI, czasy realizacji, koszty, jakość, SLA, wąskie gardła, punkty decyzyjne i ryzyka operacyjne.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
7.	Narzędzia wspomagające modelowanie i zarządzanie procesami: edytory BPMN, repozytoria modeli, systemy workflow/BPMS oraz podstawy zarządzania wersjami dokumentacji procesowej.	W1, W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
8.	Nowoczesne podejścia do zarządzania procesami: process mining, automatyzacja RPA, integracja procesów z systemami ERP/CRM, analiza danych procesowych i monitorowanie wykonania procesu.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
9.	Zarządzanie zmianą procesową: komunikacja z interesariuszami, uzgadnianie wymagań, prezentacja modelu, ocena wpływu zmian i przygotowanie rekomendacji wdrożeniowych.	U1, K1	Wykłady, Projekty
10.	Zarządzanie zmianą procesową: komunikacja z interesariuszami, uzgadnianie wymagań, prezentacja modelu, ocena wpływu zmian i przygotowanie rekomendacji wdrożeniowych.	W3, U1, U2, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria komputerowe	15

Projekty	15
Egzaminy i zaliczenia w sesji	4
Opracowanie sprawozdań z laboratoriów	8
Przygotowanie projektu	10
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	8
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Niezawodność i odporność systemów wieloprocesorowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04169.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria: 30 • Projekty: 15	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie zaawansowanej wiedzy dotyczącej architektur wieloprocesorowych systemów wbudowanych oraz metod zapewniania ich niezawodności i odporności na uszkodzenia.
C2	Zapoznanie studentów z mechanizmami redundancji sprzętowej i programowej oraz metodami tolerowania błędów w systemach wbudowanych i cyber-fizycznych.
C3	Przedstawienie metod projektowania, implementacji i oceny niezawodności systemów czasu rzeczywistego, procesów uruchamiania systemu oraz mechanizmów diagnostycznych.
C4	Zapoznanie studentów z problematyką niezawodnego szeregowania zadań w systemach wieloprocesorowych oraz współczesnymi metodami optymalizacji i zwiększania odporności systemów.
C5	Rozwijanie kompetencji w zakresie analizy, projektowania i eksperymentalnej oceny niezawodności, odporności oraz cyberodporności nowoczesnych systemów wbudowanych i cyber-fizycznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Zna architektury wieloprocesorowych systemów wbudowanych oraz rozumie wyzwania związane z zapewnieniem ich niezawodności i odporności na awarie.	EC2-W1, EC2-W4	Kolokwium
W2	Zna metody zwiększania odporności systemów wbudowanych wykorzystujące redundancję sprzętową i programową oraz rozumie ich wpływ na niezawodność systemu.	EC2-W1, EC2-W4	Kolokwium
W3	Zna mechanizmy zapewniania niezawodności systemów jednozadaniowych oraz systemów czasu rzeczywistego, w tym metody monitorowania i odzyskiwania poprawnego działania po wystąpieniu błędów.	EC2-W1, EC2-W4	Kolokwium
W4	Zna mechanizmy zapewniania niezawodności procesu uruchamiania systemu, diagnostyki oraz monitorowania pracy systemów wbudowanych.	EC2-W1, EC2-W4	Kolokwium
W5	Zna metody niezawodnego szeregowania zadań w systemach wieloprocesorowych oraz ich wpływ na dostępność, wydajność i odporność systemu.	EC2-W1, EC2-W4	Kolokwium
W6	Zna zagadnienia związane z odpornością systemów cyber-fizycznych oraz zależności pomiędzy niezawodnością, bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem.	EC2-W1, EC2-W4	Kolokwium
W7	Zna metody oceny, analizy i eksperymentalnej weryfikacji niezawodności systemów wieloprocesorowych.	EC2-W1, EC2-W4	Kolokwium
Umiejętności – Student/ka:			

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U1	Potrafi zaprojektować i zaimplementować wieloprocesorowy system sterowania i monitorowania z wykorzystaniem współczesnych platform systemów wbudowanych.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
U2	Potrafi projektować i implementować systemy wykorzystujące redundancję sprzętową i programową w celu zwiększenia ich odporności na awarie.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
U3	Potrafi zaprojektować i zrealizować system wyposażony w mechanizmy zapewniające niezawodność procesu uruchamiania, diagnostyki i monitorowania działania.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
U4	Potrafi projektować i implementować mechanizmy niezawodnego szeregowania zadań w wieloprocesorowych systemach wbudowanych.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
U5	Potrafi projektować, implementować oraz eksperymentalnie oceniać odporne na awarie systemy cyber-fizyczne.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
U6	Potrafi przeprowadzać analizę niezawodności systemów wieloprocesorowych oraz interpretować wyniki eksperymentów związanych z oceną ich odporności.	EC2-U3, EC2-U4	Rozwiązanie zadania problemowego, Obserwacja pracy studenta
Kompetencji społecznych – Student/ka:			
K1	Jest gotów do współpracy w zespole projektowym przy projektowaniu, implementacji i ocenie niezawodnych oraz odpornych na awarie systemów wbudowanych i cyber-fizycznych.	EC2-K2	Projekt, Obserwacja pracy studenta
K2	Jest gotów do krytycznej oceny proponowanych rozwiązań technicznych pod kątem ich niezawodności, odporności i bezpieczeństwa.	EC2-K2	Projekt, Obserwacja pracy studenta
K3	Rozumie znaczenie niezawodności i odporności systemów komputerowych w zastosowaniach przemysłowych, infrastrukturalnych oraz systemach krytycznych dla bezpieczeństwa.	EC2-K2	Projekt, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wieloprocesorowe systemy wbudowane – architektury i wyzwania niezawodnościowe.	W1	Wykłady, Wykłady synchroniczne
2.	Redundancja sprzętowa i programowa jako podstawa odporności systemów.	W2	Wykłady, Wykłady synchroniczne
3.	Niezawodność systemów jednozadaniowych i czasu rzeczywistego.	W3	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Niezawodność procesu uruchamiania systemu. Diagnostyka, monitorowanie i fault injection.	W1, W2, W3, W4, W5	Wykłady, Wykłady synchroniczne
5.	Niezawodność mechanizmów szeregowania zadań. Metaheurystyki w niezawodnym szeregowaniu zadań.	W5	Wykłady, Wykłady synchroniczne
6.	Niezawodność systemów FPGA i SoC FPGA.	W6	Wykłady, Wykłady synchroniczne
7.	Odporność, niezawodność oraz cyberbezpieczeństwo systemów cyber-fizycznych.	W6, W7	Wykłady, Wykłady synchroniczne
8.	Metody oceny niezawodności systemów wieloprocesorowych. Systemy samonaprawialne oraz współczesne kierunki badań.	W7	Wykłady, Wykłady synchroniczne
9.	Definicja problemu, analiza literatury oraz projekt architektury systemu.	W1, W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria
10.	Implementacja bazowego systemu wieloprocesorowego.	W1, W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria
11.	Implementacja mechanizmów redundancji.	W1, W2, W3, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria
12.	Implementacja mechanizmów monitorowania i odzyskiwania.	W3, W4, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria
13.	Monitorowanie i diagostyka systemów cyber-fizycznych.	W3, U1, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria
14.	Implementacja niezawodnego szeregowania.	W5, U4	Wykłady, Wykłady synchroniczne, Laboratoria
15.	Implementacja i ocena metod optymalizacji.	W5, U4	Wykłady, Wykłady synchroniczne, Laboratoria
16.	Eksperymenty i pomiary niezawodności.	W6, W7, U5, U6	Wykłady, Wykłady synchroniczne, Laboratoria
17.	Projekt, implementacja i eksperymentalna ocena odpornego na błędy cyber-fizycznego systemu wieloprocesorowego wykorzystującego wybrane mechanizmy niezawodności, odporności i cyberbezpieczeństwa.	W1, W2, W3, W4, W5, W6, W7, U1, U2, U3, U4, U5, U6, K1, K2, K3	Wykłady, Wykłady synchroniczne, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15

Laboratoria	30
Projekty	15
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10
Przygotowanie projektu	24
Konsultacje przedmiotowe	2
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Programowanie robotów przemysłowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04170.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 10, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 10 • Laboratoria: 40 • Projekty: 10	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie studentom wiadomości dotyczących metodologii programowania robotów przemysłowych oraz zna przykładowe środowisko programowania robotów.
C2	Zapoznanie studentów ze stanowiskiem dydaktycznym, składającym się z robota, sterownika i panelu nauczania ze szczególnym uwzględnieniem zasad bezpieczeństwa oraz zasadami pracy z robotem.
C3	Nauczenie studentów podstaw programowania operacji i ruchu robotów przemysłowych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje metodologię i techniki programowania wybranych typów robotów.	EC2-W6	Zaliczenie pisemne
Umiejętności – Student/ka:			
U1	obsługuje robota przemysłowego oraz związane z nim urządzenia sterujące i programujące.	EC2-U3, EC2-U9	Obserwacja pracy studenta
U2	posługuje się językiem programowania na poziomie podstawowym, umożliwiającym programowanie ruchu i operacji robota.	EC2-U3, EC2-U9	Obserwacja pracy studenta
Kompetencji społecznych – Student/ka:			
K1	współpracuje w zespole, przyjmuje różne role i bierze odpowiedzialność za realizację wspólnych zadań ze szczególnym uwzględnieniem zasad BHP podczas pary z robotem.	EC2-K2	Projekt, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Metody i charakterystyka programowania robotów. Podstawy teoretyczne programowania robotów.	W1	Wykłady, Wykłady synchroniczne
2.	Architektura sterownika robota. Wybrany panel nauczania robota. Wybrane środowisk/o/a programowania robotów.	W1	Wykłady, Wykłady synchroniczne
3.	Zasady BHP dotyczące programowania robotów. Struktura i funkcje stanowiska dydaktycznego do programowania robotów. Metody operowania robotem przy pomocy panelu operatorskiego i bezpieczeństwo obsługi robota.	W1, U1, U2, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty
4.	Zasady pracy z Nawigatorem. Ruch robota w układach współrzędnych. Obciążanie robota. Kalibracja robota. Ruch pomiędzy zadanymi punktami w przestrzeni. Realizacja funkcji ruchu, w tym sklejanych (spline). Techniki programowania operacji uchwytów.	W1, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	10
Laboratoria	40

Projekty	10
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	36
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Bezpieczeństwo aplikacji webowych i mobilnych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04171.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 30	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Poznanie aktualnego krajobrazu zagrożeń dotyczących aplikacji webowych i mobilnych oraz obowiązującymi standardami bezpieczeństwa (OWASP, NIST, ISO 27001).
C2	Wykształcenie umiejętności identyfikowania, analizowania i eksploatowania podatności w aplikacjach webowych i mobilnych z wykorzystaniem profesjonalnych narzędzi i metodyk.
C3	Przygotowanie do projektowania i wdrażania mechanizmów obronnych zgodnych z zasadą "security by design" w cyklu życia oprogramowania.
C4	Rozwinięcie kompetencji w zakresie przeprowadzania audytów bezpieczeństwa i sporządzania profesjonalnej dokumentacji zgodnej ze standardami branżowymi.
C5	Kształtowanie postaw etycznych w obszarze bezpieczeństwa IT oraz świadomości odpowiedzialnego ujawniania podatności (Responsible Disclosure).

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	zna i rozumie mechanizmy działania najważniejszych klas podatności aplikacji webowych i mobilnych (zgodnie z OWASP Top 10 Web i Mobile), rozumie techniki ich eksploatacji oraz zna metody i dobre praktyki ich mitygacji, a także posiada wiedzę na temat standardów i norm regulujących bezpieczeństwo oprogramowania.	EC2-W2, EC2-W6	Kolokwium
Umiejętności – Student/ka:			
U1	potrafi samodzielnie przeprowadzić audyt bezpieczeństwa aplikacji webowej lub mobilnej z zastosowaniem profesjonalnych metodyk i narzędzi (SAST, DAST, pentesting), prawidłowo ocenić ryzyko wykrytych podatności z użyciem systemu CVSS oraz opracować raport z audytu zawierający rekomendacje naprawcze.	EC2-U3, EC2-U4, EC2-U6	Kolokwium, Projekt
Kompetencji społecznych – Student/ka:			
K1	jest świadomy etycznych i prawnych aspektów działań w obszarze bezpieczeństwa aplikacji, rozumie znaczenie zasad Responsible Disclosure, potrafi pracować w zespole przy realizacji projektu audytu bezpieczeństwa oraz odpowiedzialnie zarządza informacją o znalezionych podatnościach.	EC2-K3	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawy bezpieczeństwa aplikacji: model CIA, standardy (OWASP, NIST, ISO 27001), cykl życia bezpiecznego oprogramowania (SDL, SAMM), terminologia. OWASP Web Top 10 – analiza klas podatności: Injection, Broken Authentication, Sensitive Data Exposure, XXE, Broken Access Control, Security Misconfiguration, XSS, Insecure Deserialization, Known Vulnerabilities, Logging & Monitoring.	W1	Wykłady, Wykłady synchroniczne
2.	Bezpieczeństwo API (REST, GraphQL, WebSocket): OWASP API Security Top 10, autentykacja i autoryzacja (OAuth 2.0, OpenID Connect, JWT), BOLA, Mass Assignment, Rate Limiting. Bezpieczeństwo aplikacji mobilnych (Android i iOS): OWASP Mobile Top 10, sandbox, uprawnienia, bezpieczne przechowywanie danych, analiza ruchu sieciowego, reverse engineering.	W1	Wykłady, Wykłady synchroniczne
3.	Kryptografia stosowana: TLS/HTTPS, Certificate Pinning, bezpieczne uwierzytelnianie (bcrypt, Argon2, MFA, FIDO2/WebAuthn), zarządzanie sesją, JWT – podatności.	W1	Wykłady, Wykłady synchroniczne
4.	Testowanie bezpieczeństwa i DevSecOps: SAST, DAST, IAST, SCA, pentesting; narzędzia (Burp Suite, ZAP, SonarQube, Snyk); CI/CD security pipeline; Threat Modeling (STRIDE, PASTA).	W1	Wykłady, Wykłady synchroniczne
5.	Konfiguracja środowiska laboratoryjnego: Kali Linux, Docker, DVWA, WebGoat, Juice Shop; obsługa Burp Suite i OWASP ZAP. Praktyczna eksploatacja podatności Injection (SQL Injection, SQLMap) i Cross-Site Scripting (Stored, Reflected, DOM); konfiguracja CSP.	U1	Laboratoria komputerowe
6.	Ataki na mechanizmy uwierzytelniania i sesji: brute-force, Session Hijacking, analiza i fałszowanie tokenów JWT, CSRF. Testowanie bezpieczeństwa API REST: rekonesans Swagger/OpenAPI, testowanie IDOR/BOLA, Mass Assignment, automatyczne skanowanie API.	U1	Laboratoria komputerowe
7.	Statyczna i dynamiczna analiza aplikacji mobilnych: analiza APK, SSL Pinning bypass (Frida), analiza lokalnego przechowywania danych. Skanowanie podatności: OWASP ZAP Full Scan, Nikto; SAST (SonarQube, Semgrep, Bandit); SCA (OWASP Dependency-Check, Snyk); ocena CVSS.	U1	Laboratoria komputerowe
8.	Ćwiczenia CTF z zakresu Web & Mobile Security: scenariusze SQL Injection, XSS, IDOR, JWT attacks, LFI/RFI, SSRF, deserialization.	U1	Laboratoria komputerowe
9.	Planowanie i przygotowanie audytu bezpieczeństwa – omówienie wymagań projektu, organizacja zespołów, wybór aplikacji, analiza dokumentacji i kodu źródłowego, modelowanie zagrożeń (STRIDE), identyfikacja powierzchni ataku oraz przygotowanie architektury i harmonogramu prac.	U1, K1	Projekty

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
10.	Przeprowadzenie testów bezpieczeństwa aplikacji i infrastruktury – rekonesans, mapowanie aplikacji, testy podatności (m.in. Injection, XSS, IDOR/BOLA, SSRF, XXE), analiza API, uwierzytelniania, autoryzacji, konfiguracji serwerów oraz bezpieczeństwa aplikacji mobilnych i webowych.	U1, K1	Projekty
11.	Analiza wyników i ocena ryzyka – weryfikacja wykrytych podatności, eliminacja fałszywych alarmów, przygotowanie dowodów eksploatacji, ocena wpływu biznesowego oraz klasyfikacja ryzyka zgodnie z CVSS.	U1, K1	Projekty
12.	Raportowanie i prezentacja rezultatów – opracowanie raportu z audytu wraz z rekomendacjami naprawczymi, priorytetyzacja działań remediacyjnych, prezentacja wyników, demonstracja testów oraz dyskusja i podsumowanie projektów.	U1, K1	Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria komputerowe	15
Projekty	30
Egzaminy i zaliczenia w sesji	4
Konsultacje przedmiotowe	11
Przygotowanie projektu	10
Studiowanie literatury przedmiotu	10
Przygotowanie się do kolokwiów i egzaminów	5
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Kryptografia

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04172.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma prowadzenia i godziny zajęć** • Wykłady: 10, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 10 • Laboratoria komputerowe: 30	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z podstawowymi pojęciami, modelami i metodami współczesnej kryptografii, w szczególności z mechanizmami zapewniania poufności, integralności, uwierzytelniania oraz niezaprzeczalności informacji. Przedstawienie matematycznych podstaw kryptografii oraz zasad działania algorytmów kryptografii symetrycznej, asymetrycznej i funkcji skrótu
C2	Rozwijanie umiejętności analizy i oceny bezpieczeństwa mechanizmów kryptograficznych poprzez rozwiązywanie zadań problemowych dotyczących generowania kluczy, szyfrowania i deszyfrowania danych, tworzenia podpisów cyfrowych, wymiany kluczy oraz identyfikacji podatności wynikających z niewłaściwego doboru lub implementacji algorytmów kryptograficznych.
C3	Zapoznanie studentów z praktycznymi aspektami stosowania kryptografii w systemach informatycznych poprzez realizację ćwiczeń laboratoryjnych obejmujących wykorzystanie bibliotek kryptograficznych, konfigurację infrastruktury klucza publicznego (PKI), generowanie i weryfikację certyfikatów cyfrowych, analizę protokołów TLS/SSL, SSH oraz implementację mechanizmów ochrony danych.
C4	Rozwijanie kompetencji w zakresie projektowania i wdrażania rozwiązań kryptograficznych wspierających bezpieczeństwo systemów teleinformatycznych, z wykorzystaniem narzędzi programistycznych i środowisk eksperymentalnych, a także kształtowanie umiejętności oceny skuteczności zabezpieczeń kryptograficznych, zarządzania kluczami oraz analizy współczesnych zagrożeń i ataków kryptograficznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	definiuje podstawowe pojęcia z zakresu kryptografii, w tym poufność, integralność, uwierzytelnianie, niezaprzeczalność, tekst jawny, szyfrogram, klucz kryptograficzny, funkcję skrótu, podpis cyfrowy oraz certyfikat cyfrowy, objaśnia podstawowe zasady działania algorytmów kryptografii symetrycznej i asymetrycznej, opisuje rolę funkcji skrótu, kodów MAC oraz mechanizmów wymiany kluczy, a także charakteryzuje podstawowe cele stosowania kryptografii w systemach teleinformatycznych i cyberbezpieczeństwie.	EC2-W3	Egzamin pisemny, Test
W2	posiada uporządkowaną wiedzę w zakresie zasad działania i zastosowań podstawowych algorytmów oraz protokołów kryptograficznych, w tym AES, RSA, Diffie-Hellmana, ECC, SHA, HMAC, podpisu cyfrowego, PKI, TLS/SSL oraz SSH, zna podstawowe zagrożenia i ataki kryptograficzne, w tym ataki brute force, słownikowe, urodzinowe, Man-in-the-Middle, padding oracle oraz side-channel attacks, rozumie zasady zarządzania kluczami kryptograficznymi, doboru długości kluczy, stosowania certyfikatów cyfrowych oraz interpretacji poziomu bezpieczeństwa rozwiązań kryptograficznych w praktycznych systemach informatycznych.	EC2-W3	Egzamin pisemny, Odpowiedź ustna, Test
Umiejętności – Student/ka:			

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U1	potrafi analizować i dobierać mechanizmy kryptograficzne do określonych zastosowań w systemach teleinformatycznych, stosując odpowiednie algorytmy szyfrowania, funkcje skrótu, mechanizmy uwierzytelniania oraz podpisu cyfrowego, umie przeprowadzać operacje generowania kluczy, szyfrowania i deszyfrowania danych, weryfikacji integralności informacji oraz uwierzytelniania użytkowników, interpretować uzyskane wyniki oraz oceniać poziom bezpieczeństwa zastosowanych rozwiązań kryptograficznych z uwzględnieniem potencjalnych zagrożeń i podatności.	EC2-U5	Kolokwium, Odpowiedź ustna
U2	potrafi dobierać, konfigurować i stosować mechanizmy kryptograficzne służące ochronie danych i komunikacji w systemach teleinformatycznych, generować i zarządzać kluczami kryptograficznymi, wykorzystywać certyfikaty cyfrowe oraz infrastrukturę klucza publicznego, a także oceniać poprawność i bezpieczeństwo wdrożonych rozwiązań kryptograficznych.	EC2-U5	Kolokwium, Odpowiedź ustna
Kompetencji społecznych – Student/ka:			
K1	jest gotów do odpowiedzialnego stosowania mechanizmów kryptograficznych w ochronie informacji, ma świadomość znaczenia poufności, integralności i autentyczności danych oraz rozumie konsekwencje wynikające z niewłaściwego projektowania, implementacji lub użytkowania rozwiązań kryptograficznych dla bezpieczeństwa systemów teleinformatycznych i ich użytkowników.	EC2-K2	Odpowiedź ustna, Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do kryptografii: podstawowe pojęcia, cele kryptografii, poufność, integralność, uwierzytelnianie, niezaprzeczalność, model przeciwnika, zasada Kerckhoffsa.	W1, K1	Wykłady, Wykłady synchroniczne
2.	Podstawy matematyczne kryptografii: arytmetyka modularna, kongruencje, algorytm Euklidesa, odwrotność modularna, potęgowanie modularne, liczby pierwsze, funkcja Eulera.	W1	Wykłady, Wykłady synchroniczne
3.	Kryptografia klasyczna: szyfry podstawieniowe i przestawieniowe, szyfr Cezara, Vigenère’a, analiza częstości, znaczenie kryptografii klasycznej dla współczesnych metod ochrony informacji.	W1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
4.	Kryptografia symetryczna: szyfry strumieniowe i blokowe, DES, 3DES, AES, struktura algorytmu AES, długości kluczy, podstawowe właściwości i zastosowania szyfrów symetrycznych.	W1, W2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
5.	Tryby pracy szyfrów blokowych: ECB, CBC, CFB, OFB, CTR, GCM, wektor inicjalizujący, nonce, szyfrowanie uwierzytelnione, typowe błędy stosowania trybów pracy.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
6.	Funkcje skrótu i integralność danych: właściwości funkcji skrótu, MD5, SHA-1, SHA-2, SHA-3, odporność na kolizje, atak urodzinowy, zastosowanie funkcji skrótu w cyberbezpieczeństwie.	W1, W2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
7.	Przechowywanie haseł i funkcje wyprowadzania klucza: salt, pepper, PBKDF2, bcrypt, scrypt, Argon2, ataki słownikowe, rainbow tables, zasady bezpiecznego przechowywania haseł.	W2, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
8.	Kody uwierzytelniające wiadomości: MAC, HMAC, CMAC, AEAD, różnica między funkcją skrótu a kodem MAC, zastosowanie mechanizmów uwierzytelniania wiadomości w systemach informatycznych.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
9.	Kryptografia asymetryczna: idea klucza publicznego i prywatnego, RSA, generowanie kluczy, szyfrowanie, deszyfrowanie, podpisywanie, padding OAEP i PSS, ograniczenia i typowe błędy stosowania RSA.	W1, W2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
10.	Wymiana kluczy kryptograficznych: Diffie-Hellman, ECDH, atak Man-in-the-Middle, Perfect Forward Secrecy, uzgadnianie kluczy w protokołach komunikacyjnych.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
11.	Kryptografia krzywych eliptycznych: podstawowe pojęcia ECC, ECDSA, EdDSA, Ed25519, zalety kryptografii eliptycznej, zastosowania w systemach mobilnych, IoT i komunikacji sieciowej.	W2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
12.	Podpis cyfrowy i infrastruktura klucza publicznego: podpis cyfrowy, certyfikaty X.509, urzędy certyfikacji, łańcuch zaufania, CSR, CRL, OCSP, certyfikaty serwerowe i klienckie.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
13.	Protokoły kryptograficzne: TLS 1.2/1.3, SSH, IPsec, PGP/GPG, Kerberos, zastosowanie protokołów kryptograficznych w ochronie komunikacji sieciowej i usług internetowych.	W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
14.	Zarządzanie kluczami kryptograficznymi: generowanie, przechowywanie, rotacja, dystrybucja i niszczenie kluczy, HSM, TPM, KMS, zarządzanie sekretami w systemach informatycznych i chmurowych.	W2, U2, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	10
Laboratoria komputerowe	30

Egzaminy i zaliczenia w sesji	4
Opracowanie sprawozdań z laboratoriów	16
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	15
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Programowanie defensywne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04173.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30 • Laboratoria komputerowe: 20 • Projekty: 20	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Celem zajęć jest zapoznanie studentów z zasadami projektowania i implementacji oprogramowania odpornego na błędy, niepoprawne dane wejściowe oraz nieprzewidziane sytuacje w środowisku wykonawczym. Studenci nabędą umiejętność stosowania technik programowania defensywnego, w tym walidacji danych, obsługi wyjątków, asercji, zabezpieczania interfejsów oraz tworzenia kodu o wysokiej niezawodności i bezpieczeństwie. Szczególny nacisk położony zostanie na identyfikację potencjalnych zagrożeń oraz minimalizowanie ryzyka wystąpienia błędów w systemach informatycznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	posiada pogłębioną wiedzę i rozumie znaczenie zagrożeń dla bezpieczeństwa wynikających z występowania defektów w oprogramowaniu.	EC2-W6	Projekt, Sprawozdanie, Zaliczenie pisemne
W2	posiada wiedzę i rozumie standardy oraz dobre praktyki związane z wykrywaniem, usuwaniem i zapobieganiem defektom prowadzącym do powstawania podatności w oprogramowaniu.	EC2-W6	Projekt, Sprawozdanie, Zaliczenie pisemne
W3	posiada wiedzę i rozumie standardy tworzenia bezpiecznego oprogramowania oraz zasady opracowywania modeli zagrożeń dla systemów informatycznych.	EC2-W6	Projekt, Sprawozdanie, Zaliczenie pisemne
Umiejętności – Student/ka:			
U1	potrafi opracować model zagrożeń dla oprogramowania oraz stosować zasady bezpiecznego kodowania w procesie jego wytwarzania.	EC2-U6	Projekt, Sprawozdanie, Zaliczenie pisemne
Kompetencji społecznych – Student/ka:			
K1	jest gotów do ciągłego aktualizowania wiedzy oraz rozwijania umiejętności w zakresie tworzenia bezpiecznego oprogramowania.	EC2-K2	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Defekty w oprogramowaniu związane z bezpieczeństwem - charakterystyka i klasyfikacja defektów wpływających na bezpieczeństwo systemów informatycznych. Przegląd najczęściej występujących podatności (m.in. błędy walidacji danych, przepełnienia bufora, podatności typu injection, błędy uwierzytelniania i autoryzacji). Wprowadzenie do modeli zagrożeń – identyfikacja zasobów, aktorów zagrożeń, wektorów ataku oraz potencjalnych scenariuszy nadużyć. Analiza wpływu defektów na poufność, integralność i dostępność danych (CIA triad).	W1, W2, W3, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
2.	Wykrywanie podatności - metody identyfikacji błędów i podatności w oprogramowaniu. Przegląd technik przeglądu kodu (code review), w tym przeglądów manualnych i automatycznych. Wykorzystanie narzędzi analizy statycznej i dynamicznej (SAST/DAST) do wykrywania podatności na wczesnych etapach cyklu życia oprogramowania. Rola testów jednostkowych, integracyjnych i bezpieczeństwa w procesie zapewniania jakości oraz bezpieczeństwa kodu. Wprowadzenie do testów fuzzingowych i analizy pokrycia kodu.	W1, W2, W3, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
3.	Usuwanie podatności i zapobieganie im - techniki eliminowania wykrytych podatności oraz strategie zapobiegania ich powstawaniu. Zasady programowania defensywnego i elementy podejścia ofensywnego (myślenie jak atakujący). Przegląd standardów i wytycznych tworzenia bezpiecznego oprogramowania (np. OWASP, CERT, SEI). Dobre praktyki w zakresie walidacji danych, zarządzania błędami, bezpiecznej obsługi wyjątków oraz kontroli dostępu. Znaczenie bezpiecznego cyklu życia oprogramowania (SSDLC) oraz automatyzacji procesów bezpieczeństwa w pipeline'ach CI/CD.	W1, W2, W3, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	30
Laboratoria komputerowe	20
Projekty	20
Egzaminy i zaliczenia w sesji	4
Przygotowanie sprawozdań, raportów, projektów, prezentacji	10
Przygotowanie się do kolokwiów i egzaminów	16
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Bezpieczeństwo infrastruktury krytycznej

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.21.04174.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria: 45	5

Cele kształcenia dla zajęć

Kod	Cel
C1	Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Zna systemy i infrastrukturę krytyczną i kluczową	EC2-W11, EC2-W2, EC2-W4	Rozwiązanie zadania problemowego, Sprawozdanie
Umiejętności – Student/ka:			
U1	Potrafi identyfikować zagrożenia na jakie narażone są systemu IK	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego, Sprawozdanie
U2	Potrafi wykrywać i analizować zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego, Sprawozdanie
U3	Potrafi dobrać rodzaj i zakres działań naprawczych	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego, Sprawozdanie
U4	Jest przygotowany do zarządzania i administrowania takimi systemami	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	Potrafi zidentyfikować i zapobiegać zagrożeniom wpływającym na społeczeństwo i obywateli	EC2-K2, EC2-K4	Rozwiązanie zadania problemowego, Sprawozdanie

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Zagadnienia związane z Infrastrukturą krytyczną	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
2.	Zagadnienia związane z Infrastrukturą kluczową	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
3.	Krajowy system cyberbezpieczeństwa związany z infrastrukturą IJ	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
4.	Omówienie i analiza Ustawy o Krajowym systemie cyberbezpieczeństwa	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
5.	NIS 1 i NIS 2 – omówienie dyrektyw UE w zakresie Cyberbezpieczeństwa	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
6.	Zasady projektowania i budowy odpornych systemów informatycznych zgodnych z KSC	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
7.	Analiza i obsługa incydentów i podatności.	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne
8.	Budowanie schematów systemów bezpieczeństwa IK	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne, Laboratoria

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
9.	Analiza struktur organizacyjnych i projektowanie bezpieczeństwa IK	W1, U1, U2, U3, U4, K1	Wykłady, Wykłady synchroniczne, Laboratoria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria	45
Egzaminy i zaliczenia w sesji	4
Symulacje komputerowe	10
Opracowanie sprawozdań z laboratoriów	21
Opracowanie wyników	20
Przygotowanie prezentacji multimedialnej	10
Łączny nakład pracy studenta	**Liczba godzin** 125
Liczba punktów ECTS	**ECTS** 5

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Społeczne aspekty cyberbezpieczeństwa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04165.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty humanistyczne i społeczne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Analiza społecznych, psychologicznych, kulturowych i etycznych aspektów cyberbezpieczeństwa.
C2	Rozwijanie kompetencji krytycznej oceny zagrożeń występujących w środowisku cyfrowym.
C3	Kształtowanie odpowiedzialności społecznej związanej z projektowaniem i wdrażaniem technologii informacyjnych.
C4	Przygotowanie do identyfikowania społecznych konsekwencji cyberataków, dezinformacji oraz nadużyć technologicznych.
C5	Rozwijanie kompetencji związanych z ochroną prywatności, praw człowieka i bezpieczeństwa informacyjnego.
C6	Kształtowanie postawy inżyniera jako lidera społecznego odpowiedzialnego za bezpieczeństwo cyfrowe społeczeństwa.
C7	Wspieranie uczenia się przez całe życie w obszarze cyberbezpieczeństwa i nowych technologii.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje społeczne i kulturowe uwarunkowania cyberbezpieczeństwa.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
W2	opisuje mechanizmy oddziaływania technologii cyfrowych na zachowania jednostek i grup społecznych.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
W3	identyfikuje społeczne zagrożenia wynikające z cyberprzemocy, dezinformacji i manipulacji informacyjnej.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
W4	określa zależności między cyberbezpieczeństwem, ochroną prywatności i prawami człowieka.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
W5	charakteryzuje znaczenie cyberbezpieczeństwa dla funkcjonowania instytucji demokratycznych i społeczeństwa obywatelskiego.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
W6	opisuje społeczne konsekwencje rozwoju sztucznej inteligencji oraz automatyzacji procesów decyzyjnych.	EC2-W10, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
Umiejętności – Student/ka:			
U1	analizuje społeczne skutki incydentów cyberbezpieczeństwa.	EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U2	interpretuje przypadki naruszeń bezpieczeństwa cyfrowego z perspektywy społecznej i etycznej.	EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
U3	ocenia wpływ rozwiązań technologicznych na bezpieczeństwo użytkowników.	EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
U4	opracowuje rekomendacje dotyczące budowania kultury cyberbezpieczeństwa.	EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
U5	wykorzystuje argumentację opartą na danych podczas debat dotyczących bezpieczeństwa cyfrowego.	EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
Kompetencji społecznych – Student/ka:			
K1	uwzględnia społeczne konsekwencje wdrażanych technologii.	EC2-K3, EC2-K5	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
K2	uczestniczy w debatach dotyczących odpowiedzialnego wykorzystania technologii cyfrowych.	EC2-K3, EC2-K5	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
K3	inicjuje działania wspierające rozwój kultury cyberbezpieczeństwa.	EC2-K3, EC2-K5	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego
K4	przyjmuje odpowiedzialność za etyczne aspekty działalności zawodowej związanej z cyberbezpieczeństwem.	EC2-K3, EC2-K5	Odpowiedź ustna, Portfolio, Prezentacja, Rozwiązanie zadania problemowego

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Moduł 1. Człowiek w cyberprzestrzeni • społeczeństwo cyfrowe, • kultura bezpieczeństwa, • cyfrowa tożsamość, • ślad cyfrowy. Aktywności studentów: analiza materiałów wizualnych, karta pracy „Mój cyfrowy profil”, dyskusja problemowa. Metody: Interactive Lecture, Think–Pair–Share.	W1, W5, U1, K1	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
2.	Moduł 2. Psychologia cyberzagrożeń • inżynieria społeczna, • heurystyki poznawcze, • phishing, • manipulacja emocjonalna. Aktywności studentów: analiza rzeczywistych kampanii phishingowych, identyfikacja technik manipulacyjnych. Metody: Case Study, Problem-Based Learning.	W2, U2, K2	Wykłady, Wykłady synchroniczne
3.	Moduł 3. Dezinformacja, fake news i wojna informacyjna • fake news, • propaganda cyfrowa • algorytmy rekomendacyjne, • polaryzacja społeczna. Aktywności studentów: analiza materiałów medialnych, karta pracy „Jak rozpoznać manipulację?”. Metody: Inquiry-Based Learning, debata oksfordzka.	W3, U3, U5, K3	Wykłady, Wykłady synchroniczne
4.	Moduł 4. Prywatność, dane i prawa człowieka • prywatność cyfrowa, • profilowanie użytkowników, • kapitalizm nadzoru, • etyka danych. Aktywności studentów: analiza studiów przypadków, dyskusja konwersatoryjna. Metody: Challenge-Based Learning.	W4, U4, K4	Wykłady, Wykłady synchroniczne
5.	Moduł 5. Cyberprzemoc i dobrostan cyfrowy • cyberbullying, • mowa nienawiści, • uzależnienia cyfrowe, • zdrowie psychiczne. Aktywności studentów: analiza materiałów filmowych, opracowanie rekomendacji profilaktycznych. Metody: Design Thinking, analiza przypadku.	W5, W6, U4, K4	Wykłady, Wykłady synchroniczne
6.	Moduł 6. Sztuczna inteligencja a bezpieczeństwo społeczne • deepfake, • generatywna AI, • odpowiedzialność algorytmiczna, automatyzacja decyzji. Aktywności studentów: analiza materiałów multimedialnych, karta pracy „AI a odpowiedzialność społeczna”. Metody: Futures Literacy, World Café.	W4, W6, U4, K4	Wykłady, Wykłady synchroniczne
7.	Moduł 7. Cyberbezpieczeństwo a demokracja i bezpieczeństwo państwa • cyberwojny, • infrastruktura krytyczna, • bezpieczeństwo wyborów, • odporność społeczna. Aktywności studentów: analiza scenariuszy przyszłości, dyskusja ekspercka. Metody: Scenario Planning.	W4, U3, K3	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
8.	Moduł 8. Projektowanie kultury cyberbezpieczeństwa • edukacja cyfrowa, • kampanie społeczne, • odpowiedzialność obywatelska. Aktywności studentów: opracowanie projektu edukacyjnego, prezentacja rezultatów. Metody: Project-Based Learning, Design Thinking.	W5, U3, K3	Wykłady, Wykłady synchroniczne

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	30
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	8
Przygotowanie sprawozdań, raportów, projektów, prezentacji	8
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Etyka w cyberbezpieczeństwie

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04166.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty humanistyczne i społeczne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Analiza społecznych, kulturowych i psychologicznych uwarunkowań cyberbezpieczeństwa.
C2	Rozwijanie kompetencji umożliwiających identyfikowanie zagrożeń wynikających z funkcjonowania człowieka w środowisku cyfrowym.
C3	Kształtowanie krytycznego podejścia do technologii informacyjnych i komunikacyjnych.
C4	Przygotowanie do projektowania rozwiązań uwzględniających bezpieczeństwo użytkowników oraz ochronę praw człowieka.
C5	Rozwijanie kompetencji związanych z odpowiedzialnym uczestnictwem w społeczeństwie cyfrowym.
C6	Wzmacnianie świadomości znaczenia cyberbezpieczeństwa dla demokracji, bezpieczeństwa państwa i zrównoważonego rozwoju.
C7	Przygotowanie do uczenia się przez całe życie w obszarze dynamicznie rozwijających się technologii cyfrowych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje społeczne i kulturowe uwarunkowania cyberbezpieczeństwa.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
W2	opisuje mechanizmy wpływu technologii cyfrowych na zachowania jednostek i grup społecznych.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
W3	identyfikuje zagrożenia wynikające z dezinformacji, manipulacji informacyjnej oraz cyberprzemocy.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
W4	określa zależności między cyberbezpieczeństwem, ochroną prywatności i prawami człowieka.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
W5	opisuje znaczenie cyberbezpieczeństwa dla funkcjonowania społeczeństwa demokratycznego.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
W6	charakteryzuje społeczne konsekwencje rozwoju sztucznej inteligencji i automatyzacji procesów decyzyjnych.	EC2-W11, EC2-W12	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
Umiejętności – Student/ka:			
U1	analizuje społeczne skutki incydentów cyberbezpieczeństwa.	EC2-U11, EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
U2	ocenia konsekwencje technologicznych rozwiązań dla bezpieczeństwa użytkowników.	EC2-U11, EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U3	interpretuje przypadki naruszeń bezpieczeństwa w kontekście społecznym i etycznym.	EC2-U11, EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
U4	opracowuje rekomendacje dotyczące bezpiecznego funkcjonowania w środowisku cyfrowym.	EC2-U11, EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
U5	wykorzystuje argumentację opartą na danych podczas debat dotyczących cyberbezpieczeństwa.	EC2-U11, EC2-U13	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
Kompetencji społecznych – Student/ka:			
K1	uwzględnia społeczne skutki wdrażanych rozwiązań technologicznych.	EC2-K3	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
K2	uczestniczy w debacie dotyczącej bezpieczeństwa cyfrowego oraz ochrony praw obywatelskich.	EC2-K3	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
K3	inicjuje działania wspierające kulturę bezpieczeństwa cyfrowego.	EC2-K3	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne
K4	przyjmuje odpowiedzialność za etyczne aspekty projektowania i wdrażania technologii.	EC2-K3	Odpowiedź ustna, Portfolio, Prezentacja, Projekt, Zaliczenie ustne

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Moduł 1. Cyberbezpieczeństwo jako problem społeczny • społeczeństwo cyfrowe, • kultura bezpieczeństwa, • człowiek jako najsłabsze i najsilniejsze ogniwo systemu. Aktywności studentów: analiza materiałów wizualnych, mapa zagrożeń społecznych, karta pracy „Moje cyfrowe ślady”. Metody: Interactive Lecture, Think–Pair–Share	W1, U1, K1	Wykłady, Wykłady synchroniczne
2.	Moduł 2. Psychologia cyberzagrożeń· • inżynieria społeczna, • phishining, • manipulacja poznawcza, • heurystyki i błędy poznawcze. Aktywności studentów: analiza rzeczywistych ataków, ćwiczenia rozpoznawania manipulacji. Metody: Case Study, Problem-Based Learning.	W2, U2, K2	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
3.	Moduł 3. Media społecznościowe, algorytmy i dezinformacja· • fake news, • bańki informacyjne, • polaryzacja społeczna, • ekonomia uwagi. Aktywności studentów: analiza materiałów medialnych, karta pracy dotycząca dezinformacji. Metody: Inquiry-Based Learning, Debata oksfordzka.	W3, U3, K3	Wykłady, Wykłady synchroniczne
4.	Moduł 4. Prywatność i prawa człowieka w świecie cyfrowym· • ochrona danych osobowych, • nadzór cyfrowy, • profilowanie użytkowników, • etyka danych. Aktywności studentów: analiza przypadków, dyskusja problemowa. Metody: Challenge-Based Learning	W4, U4, K3	Wykłady, Wykłady synchroniczne
5.	Moduł 5. Cyberprzemoc i bezpieczeństwo psychiczne • cyberbullying, • mowa nienawiści, • uzależnienia cyfrowe, • dobrostan cyfrowy. Aktywności studentów: analiza filmów pronlemowych, opracowanie rekomendacji profilaktycznych. Metody: Design Thinking, analiza przypadku.	W5, U4, U5, K3, K4	Wykłady, Wykłady synchroniczne
6.	Moduł 6. Sztuczna inteligencja a bezpieczeństwo społeczne • deepfake, • generatywna AI, • automatyzacja decyzji, • odpowiedzialność algorytmiczna. Aktywności studentów: analiza przykładów, projektowanie zasad odpowiedzialnego wykorzystania AI. Metody: Futures Literacy, World Café.	W5, W6, U4, U5, K3, K4	Wykłady, Wykłady synchroniczne
7.	Moduł 7. Cyberbezpieczeństwo a demokracja i zrównoważony rozwój • cyberwojny, • bezpieczeństwo państwa, • infrastruktura krytyczna, • SDGs a cyberbezpieczeństwo. Aktywności studentów: analiza scenariuszy przyszłości, dyskusja ekspercka. Metody: Scenario Planning, Challenge-Based Learning.	W4, W5, W6, U3, U5, K2, K4	Wykłady, Wykłady synchroniczne
8.	Moduł 8. Podsumowanie – projekt społeczny • kultura cyberbezpieczeństwa. Aktywności studentów: opracowanie kampanii edukacyjnej, prezentacja rezultatów. Metody: Project-Based Learning, Design Thinking.	W4, W5, U4, U5, K3	Wykłady, Wykłady synchroniczne

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć

Wykłady	30
Egzaminy i zaliczenia w sesji	2
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	8
Przygotowanie sprawozdań, raportów, projektów, prezentacji	8
Konsultacje przedmiotowe	2
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Systemy operacyjne czasu rzeczywistego

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.02071.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie uporządkowanej wiedzy z zakresu systemów operacyjnych czasu rzeczywistego, obejmującej architekturę systemu, mechanizmy zarządzania zadaniami, komunikacji oraz synchronizacji, a także ich zastosowanie w systemach wbudowanych i przemysłowych.
C2	Rozwinięcie umiejętności projektowania i implementacji aplikacji czasu rzeczywistego z wykorzystaniem mechanizmów wielozadaniowości, obsługi zdarzeń, komunikacji międzyzadaniowej oraz zarządzania zasobami.
C3	Kształtowanie umiejętności analizy i konfiguracji systemów czasu rzeczywistego z uwzględnieniem ograniczeń czasowych, deterministyczności działania oraz efektywnego wykorzystania zasobów sprzętowych.
C4	Przygotowanie do pracy zespołowej przy projektach systemów czasu rzeczywistego, obejmujących analizę wymagań, implementację oraz dokumentację rozwiązania.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje architekturę oraz zasady działania systemów operacyjnych czasu rzeczywistego, w tym mechanizmy zarządzania zadaniami, planowania, synchronizacji i komunikacji między zadaniami oraz obsługi zdarzeń i przerwań.	EC2-W1	Prezentacja, Test
W2	charakteryzuje metody projektowania systemów czasu rzeczywistego oraz wyjaśnia zasady zapewniania deterministyczności działania, rozwiązywania problemów współbieżności oraz integracji systemów czasu rzeczywistego w środowiskach wbudowanych i przemysłowych.	EC2-W1	Prezentacja, Projekt, Test
Umiejętności – Student/ka:			
U1	potrafi projektować i implementować aplikacje czasu rzeczywistego z wykorzystaniem mechanizmów wielozadaniowości, komunikacji i synchronizacji, obsługi przerwań oraz zarządzania czasem i zasobami systemu.	EC2-U3, EC2-U8	Kolokwium, Odpowiedź ustna, Projekt
Kompetencji społecznych – Student/ka:			
K1	Współpracuje w zespole projektowym, pracuje odpowiedzialnie, analizuje i ocenia przyjęte rozwiązania oraz samodzielnie rozwija wiedzę w oparciu o dokumentację techniczną i literaturę.	EC2-K2	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do systemów czasu rzeczywistego: definicje, klasy systemów, wymagania czasowe, pojęcie deterministyczności oraz obszary zastosowań w systemach wbudowanych i przemysłowych.	W1, W2	Wykłady, Wykłady synchroniczne
2.	Zarządzanie zadaniami: tworzenie i uruchamianie zadań, zadanie a wątek, priorytety, stany zadań, algorytmy planowania oraz wpływ planowania na czas reakcji systemu.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty
3.	Komunikacja i synchronizacja między zadaniami: semafory, mutexy, kolejki, zdarzenia, sekcje krytyczne oraz problemy współbieżności występujące w aplikacjach czasu rzeczywistego.	W1, W2, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty
4.	Obsługa zdarzeń i przerwań: architektura przerwań, procedury ISR, zdarzenia asynchroniczne, powiązanie przerwań z zadaniami oraz zasady projektowania reakcji systemu na zdarzenia.	W1, W2, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty
5.	Zarządzanie czasem w systemie czasu rzeczywistego: timery, opóźnienia, zadania okresowe i zdarzeniowe, wymagania czasowe oraz analiza terminowości działania aplikacji.	W1, W2, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty
6.	Problemy systemów wielozadaniowych: odwrócenie priorytetów, zakleszczenia, zagłodzenie zadań, przeciążenie systemu oraz strategie zapobiegania błędom współbieżności.	W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria
7.	Projektowanie aplikacji czasu rzeczywistego: dekompozycja funkcjonalna, dobór zadań i priorytetów, komunikacja między modułami, testowanie, debugowanie i walidacja wymagań czasowych.	W1, W2, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria	15
Projekty	15
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do kolokwiów i egzaminów	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Cyberbezpieczeństwo i analiza danych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04175.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30 • Laboratoria komputerowe: 30	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie z zaawansowanymi koncepcjami analityki bezpieczeństwa oraz paradygmatem zerowego zaufania
C2	Wykształcenie umiejętności identyfikacji śladów ataków i analizy incydentów z wykorzystaniem systemów klasy SIEM
C3	Przygotowanie do praktycznej oceny bezpieczeństwa infrastruktury i reagowania na naruszenia

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	wyjaśnia zaawansowane modele bezpieczeństwa oraz zasady architektury zerowego zaufania	EC2-W5	Test
W2	analizuje techniki ataków i mapuje je do modeli łańcucha działań intruza oraz macierzy MITRE ATT&CK	EC2-W5	Test
Umiejętności – Student/ka:			
U1	analizuje dzienniki zdarzeń, alerty oraz ruch sieciowy w celu identyfikacji incydentów bezpieczeństwa	EC2-U7	Kolokwium, Sprawozdanie
U2	przeprowadza ocenę podatności infrastruktury i interpretuje wyniki narzędzi skanujących	EC2-U1	Kolokwium, Sprawozdanie
U3	dokumentuje przebieg incydentu oraz proponuje działania ograniczające skutki naruszenia	EC2-U14	Rozwiązanie zadania problemowego, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	wykazuje gotowość do krytycznej oceny własnej wiedzy oraz odpowiedzialnego pełnienia ról zawodowych w zespole ds. bezpieczeństwa	EC2-K1, EC2-K2	Obserwacja pracy studenta

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Fundamenty analityki bezpieczeństwa i operacji obronnych. Omówienie roli centrów SOC, znaczenia telemetrii oraz ewolucji modeli ochrony w kierunku paradygmatu zerowego zaufania.	W1	Wykłady, Wykłady synchroniczne
2.	Warsztat analityka: pozyskiwanie telemetrii i badanie dzienników zdarzeń. Konfiguracja systemów w celu detekcji śladów nieautoryzowanego dostępu i weryfikacji wskaźników kompromitacji.	U1	Laboratoria komputerowe
3.	Nowoczesne systemy tożsamości i kontroli dostępu. Projektowanie rozwiązań opartych na modelach IAM/AAA, uwierzytelnianiu wieloskładnikowym oraz zaufaniu cyfrowym budowanym przez PKI.	W1	Wykłady, Wykłady synchroniczne
4.	Śledzenie aktywności intruza i mapowanie technik ataku. Praktyczne zastosowanie macierzy MITRE ATT&CK do analizy próbek szkodliwego oprogramowania i rekonstrukcji przebiegu incydentu.	U1, U3, K1	Laboratoria komputerowe
5.	Metodyka analizy ataków i profilowanie zagrożeń. Wykorzystanie ram analitycznych Cyber Kill Chain oraz MITRE ATT&CK do badania aktywności grup APT oraz kampanii ransomware.	W2	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
6.	Operacyjne wykorzystanie systemów SIEM (Wazuh/Elastic). Implementacja reguł detekcji, powiązywanie zdarzeń z wielu źródeł oraz budowa funkcjonalnych pulpitów analitycznych.	U1, U3, K1	Laboratoria komputerowe
7.	Inżynieria systemów obronnych i bezpieczeństwo infrastruktury. Wdrażanie strategii obrony w głąb, segmentacji sieci oraz mechanizmów utwardzania systemów w środowiskach chmurowych.	W1, U2	Wykłady, Wykłady synchroniczne
8.	Audyt bezpieczeństwa i identyfikacja luk infrastrukturalnych. Zautomatyzowane badanie powierzchni ataku oraz klasyfikacja podatności usług sieciowych zgodnie z modelem CVSS.	U2	Laboratoria komputerowe
9.	Zaawansowana analityka i korelacja zdarzeń w systemach klasy SIEM. Wykrywanie anomalii z użyciem wskaźników kompromitacji (IOC) oraz prezentacja danych bezpieczeństwa na pulpitach wizualizacyjnych.	W2	Wykłady, Wykłady synchroniczne
10.	Analiza śledcza ruchu sieciowego i reagowanie na naruszenia.	U1, U3, K1	Laboratoria komputerowe
11.	Kolokwium: Weryfikacja umiejętności identyfikacji incydentów, analizy dzienników oraz dokumentowania działań naprawczych.	U1, U2, U3, K1	Laboratoria komputerowe

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	30
Laboratoria komputerowe	30
Egzaminy i zaliczenia w sesji	3
Konsultacje przedmiotowe	5
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	12
Opracowanie wyników	10
Przygotowanie raportu	10
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Sztuczna inteligencja w usługach sieciowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04176.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Egzamin **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30 • Laboratoria komputerowe: 30	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Celem przedmiotu jest przekazanie studentom wiedzy i umiejętności z zakresu projektowania, integracji i oceny rozwiązań sztucznej inteligencji w usługach sieciowych. Studenci poznają architekturę nowoczesnych usług AI, sposoby wykorzystania modeli generatywnych i analitycznych w aplikacjach webowych i chmurowych, a także zasady bezpiecznego, odpowiedzialnego i efektywnego wdrażania takich rozwiązań.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	zna podstawowe pojęcia, modele i architektury sztucznej inteligencji wykorzystywanej w usługach sieciowych.	EC2-W5, EC2-W8	Zaliczenie pisemne
W2	zna zastosowania AI w obszarze przetwarzania tekstu, mowy, obrazów, dokumentów i interakcji użytkownika z systemami sieciowymi.	EC2-W5, EC2-W8	Zaliczenie pisemne
W3	zna podstawowe zagrożenia, ograniczenia i wymagania bezpieczeństwa dotyczące usług sieciowych wykorzystujących AI.	EC2-W5, EC2-W8	Zaliczenie pisemne
Umiejętności – Student/ka:			
U1	potrafi dobrać odpowiednie narzędzia i usługi AI do zadanego problemu występującego w środowisku usług sieciowych.	EC2-U10, EC2-U7	Kolokwium, Odpowiedź ustna, Sprawozdanie
U2	potrafi zaprojektować i zaimplementować prostą usługę lub aplikację sieciową wykorzystującą wybrane API lub model AI.	EC2-U10, EC2-U7	Kolokwium, Odpowiedź ustna, Sprawozdanie
U3	potrafi ocenić jakość działania rozwiązania AI oraz wskazać potencjalne problemy dotyczące bezpieczeństwa, jakości danych i wiarygodności wyników. [owasp.org], [media.defense.gov], [nist.gov]	EC2-U10, EC2-U7	Kolokwium, Odpowiedź ustna, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	jest gotów do krytycznej oceny wyników generowanych przez systemy AI oraz do odpowiedzialnego stosowania tych systemów w praktyce.	EC2-K1	Zaliczenie pisemne
K2	rozumie znaczenie etycznych, prawnych i organizacyjnych aspektów wdrażania AI w usługach sieciowych.	EC2-K1	Zaliczenie pisemne

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do sztucznej inteligencji w usługach sieciowych: podstawowe pojęcia, obszary zastosowań, przegląd współczesnych usług AI dostępnych przez API i platformy chmurowe.	W1, W2, K1, K2	Wykłady, Wykłady synchroniczne
2.	Architektura systemów AI w aplikacjach sieciowych: klient–serwer, API, mikroserwisy, usługi chmurowe, orkiestracja i integracja komponentów AI.	W1, W2, K1, K2	Wykłady, Wykłady synchroniczne
3.	Przetwarzanie języka naturalnego w usługach sieciowych: analiza tekstu, klasyfikacja, streszczanie, tłumaczenie, ekstrakcja informacji oraz modele językowe.	W1, W2, K1, K2	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Modele generatywne i ich zastosowanie w usługach sieciowych: generowanie treści, odpowiedzi dialogowych, automatyzacja interakcji oraz wspomaganie użytkownika.	W1, W2, K1, K2	Wykłady, Wykłady synchroniczne
5.	Usługi AI do przetwarzania mowy, obrazu i dokumentów: speech-to-text, text-to-speech, OCR, analiza obrazów, ekstrakcja danych z dokumentów.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
6.	Integracja AI z aplikacjami webowymi i backendowymi: wykorzystanie gotowych interfejsów API, usług platformowych oraz wzorców wdrożeniowych.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
7.	Embeddings i wyszukiwanie semantyczne: reprezentacja danych, podobieństwo semantyczne, wyszukiwanie kontekstowe i zastosowania w aplikacjach sieciowych.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
8.	Architektura RAG (Retrieval-Augmented Generation): łączenie modeli językowych z bazami wiedzy, repozytoriami dokumentów i wyszukiwaniem semantycznym.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
9.	Agenci AI i function calling: podstawy budowy systemów wykonujących operacje na podstawie poleceń użytkownika i współpracujących z usługami zewnętrznymi.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
10.	Dane w systemach AI: przygotowanie danych, jakość danych, dane nieustrukturyzowane, metadata, provenance oraz wpływ danych na skuteczność usług AI.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
11.	Ocena jakości systemów AI w usługach sieciowych: trafność odpowiedzi, halucynacje, niezawodność, wydajność, skalowalność i doświadczenie użytkownika.	W1, W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
12.	Bezpieczeństwo aplikacji AI: prompt injection, wyciek danych, nieprawidłowa obsługa odpowiedzi modelu, zagrożenia łańcucha dostaw i podatności warstwy wektorowej.	W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
13.	Ochrona danych i prywatności w usługach AI: integralność danych, zatruwanie danych, dryf danych, szyfrowanie, kontrola dostępu i monitorowanie.	W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
14.	Odpowiedzialne wdrażanie AI: governance, zarządzanie ryzykiem, zgodność z dobrymi praktykami, aspekty etyczne i organizacyjne.	W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
15.	Trendy rozwojowe i kierunki zastosowań AI w usługach sieciowych: rozwój usług generatywnych, agentowych, multimodalnych i chmurowych.	W2, W3, K1, K2	Wykłady, Wykłady synchroniczne
16.	Konfiguracja środowiska programistycznego oraz przegląd narzędzi i usług AI wykorzystywanych w aplikacjach sieciowych.	U1, U2	Laboratoria komputerowe
17.	Podstawy korzystania z interfejsów API usług AI: autoryzacja, wysyłanie zapytań, odbiór i interpretacja odpowiedz.	U1, U2	Laboratoria komputerowe

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
18.	Implementacja prostych usług przetwarzania języka naturalnego: analiza tekstu, klasyfikacja, streszczanie i tłumaczenie.	U1, U2	Laboratoria komputerowe
19.	Tworzenie aplikacji wykorzystujących modele generatywne do generowania odpowiedzi i obsługi interakcji użytkownika.	U1, U2	Laboratoria komputerowe
20.	Wykorzystanie usług przetwarzania mowy, obrazów i dokumentów w aplikacjach sieciowych	U1, U2	Laboratoria komputerowe
21.	Integracja usług AI z aplikacją webową lub backendową z użyciem gotowych bibliotek i usług chmurowych.	U1, U2, U3	Laboratoria komputerowe
22.	Przygotowanie i przetwarzanie danych wejściowych dla usług AI, w tym danych tekstowych, dokumentowych i multimedialnych.	U1, U2, U3	Laboratoria komputerowe
23.	Budowa prostego systemu wyszukiwania semantycznego z wykorzystaniem embeddingów.	U2, U3	Laboratoria komputerowe
24.	Implementacja prostego rozwiązania typu RAG z wykorzystaniem bazy wiedzy lub repozytorium dokumentów.	U2, U3	Laboratoria komputerowe
25.	Projektowanie i testowanie prostych usług agentowych lub rozwiązań opartych na function calling.	U2, U3	Laboratoria komputerowe
26.	Ocena jakości działania aplikacji AI: testowanie trafności odpowiedzi, analiza błędów i ograniczeń modeli.	U2, U3	Laboratoria komputerowe
27.	Identyfikacja podstawowych zagrożeń bezpieczeństwa w usługach AI oraz stosowanie mechanizmów ochrony danych i walidacji wyników.	U2, U3	Laboratoria komputerowe
28.	Implementacja podstawowych mechanizmów monitorowania, filtrowania treści i kontroli dostępu w aplikacjach wykorzystujących A.	U2, U3	Laboratoria komputerowe
29.	Opracowanie mini-projektu integrującego wybrane usługi AI z aplikacją sieciow.	U2, U3	Laboratoria komputerowe
30.	Prezentacja, testowanie i ocena wykonanego rozwiązania laboratoryjnego	U2, U3	Laboratoria komputerowe

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	30
Laboratoria komputerowe	30
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do kolokwiów i egzaminów	12

Opracowanie sprawozdań z laboratoriów	20
Studiowanie literatury przedmiotu	4
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Bezpieczeństwo w IoT

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04177.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria: 20 • Projekty: 20	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Poznanie typowych podatności urządzeń Internetu Rzeczy
C2	Zrozumienie kwestii transmisji danych urządzeń IoT
C3	Nabycie umiejętności zabezpieczeania urządzeń Internetu Rzeczy

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	zna typowe podatności urządzeń Internetu Rzzeczy.	EC2-W2	Kolokwium
W2	rozumie kwestie transmisji danych urządzeń IoT.	EC2-W8	Kolokwium
Umiejętności – Student/ka:			
U1	umie konfigurować zabezpieczenia urządzeń Internetu Rzeczy	EC2-U4, EC2-U8	Projekt
Kompetencji społecznych – Student/ka:			
K1	jest świadomy kluczowego znaczenia zabezpieczeń urządzeń IoT w społeczeństwie	EC2-K3	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	1. Bezpieczeństwo urządzeń Internetu Rzeczy (IoT) – analiza i przegląd stosowanych mechanizmów ochrony. 2. Prezentacja narzędzi do modelowania bezpiecznego systemu IoT. 3. Omówienie możliwych podatności oprogramowania układowego. 4. Analiza technik zabezpieczania komunikacji sieciowej w IoT. 5. Przegląd systemów IoT opartych na usługach chmurowych. 6. Protokoły transmisji bezprzewodoweji metody ich zabezpieczania.	W1, W2, K1	Wykłady, Wykłady synchroniczne
2.	1. Omówienie platformy sprzętowej używanej w trakcie zajęć. 2. Wykorzystanie narzędzi do modelowania bezpiecznego systemu IoT. 3. Poszukowanie podatności systemu w przykładowym oprogramowaniu układowym. 4. Implementacja mechanizmów bezpieczeństwa dla protokołów sieciowych w środowisku IoT. 5. Integracja systemu IoT z wybraną platformą chmurową oraz testy bezpieczeństwa. 6. Testy wybranego protokołu komunikacji bezprzewodowej.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria
3.	Projekt polegający na opracowaniu modelu urządzenia Internetu Rzeczy (IoT) oraz przeprowadzeniu analizy jego bezpieczeństwa.	U1, K1	Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć

Wykłady	15
Laboratoria	20
Projekty	20
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć	16
Przygotowanie się do kolokwiów i egzaminów	10
Przygotowanie projektu	15
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Systemy detekcji i analizy cyberzagrożeń

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04178.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Egzamin **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria: 45	4

Cele kształcenia dla zajęć

Kod	Cel
C1	zapoznanie studentów z architektura i działaniem systemów detekcji zagrożeń oraz analizy zdarzeń bezpieczeństwa w środowiskach informatycznych i przemysłowych
C2	przekazanie umiejętności w zakresie urządzeń firewall Stormshield w strukturze sieci, konfiguracji polityk bezpieczeństwa, filtrowania ruchu
C3	rozwiniecie umiejętności interpretacji danych z różnych źródeł, wyciągania wniosków operacyjnych oraz oceny skuteczności mechanizmów detekcji w kontekście ryzyka operacyjnego

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Student rozumie architektury i działanie systemów detekcji zagrożeń oraz do analizy zdarzeń bezpieczeństwa w środowiskach informatycznych i przemysłowych.	EC2-W5	Egzamin pisemny, Rozwiązanie zadania problemowego
Umiejętności – Student/ka:			
U1	Student wie jak integrować urządzenia firewall Stormshield w strukturze sieci, konfigurować polityki bezpieczeństwa, filtrować ruch.	EC2-U4, EC2-U7	Egzamin pisemny, Kolokwium, Rozwiązanie zadania problemowego
Kompetencji społecznych – Student/ka:			
K1	Student umie interpretować dane z różnych źródeł, wyciągać wnioski operacyjne oraz oceniać skuteczność mechanizmów detekcji w kontekście ryzyka organizacyjnego.	EC2-K1	Kolokwium, Rozwiązanie zadania problemowego

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	1. Wprowadzenie do cyberzagrozeń, incydentów i ich detekcji, 2. Zestawienie architektur systemów detekcji i analizy cyberzagrożeń, 3. Wskaźniki kompromitacji i wskaźniki przeciwnika, reguły detekcyjne, sygnatury i korelacja zdarzeń, 4. Opis wskaźników detekcji w środowiskach infrastruktury krytycznej, 5. Omówienie technologii logowania, monitorowania i raportowania, 6. Przedstawienie metod autentykacji, 7. Opis technologii wirtualnych sieci prywatnych VPN, IPsec, SSL,	W1, U1	Wykłady, Wykłady synchroniczne
2.	1. Wprowadzenie do stanowisk laboratoryjnych Stormshield, pierwsza konfiguracja, 2. Ustawienia interfejsow sieciowych i logowanie do planelu administratora, 3. Implementacja lańcucha ataku i rekonstrukcja incydentu, 4. Analiza logów pod kątem ataków, automatyzacja kopii zapasowych konfiguracji systemu, 5. Implementacja translacji adresów i filtrowanie ruchu, 6. Wdrozenie logowania uytkowników i autentykacji, 7. Konfiguracja wierualnej sieci VPN,	U1, K1	Laboratoria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Wykłady	15
Laboratoria	45
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	13
Opracowanie sprawozdań z laboratoriów	13
Przygotowanie się do kolokwiów i egzaminów	10
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Bezpieczeństwo systemów rozproszonych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04179.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 30	4

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z podstawowymi pojęciami, architekturami i modelami funkcjonowania systemów rozproszonych oraz zagrożeniami bezpieczeństwa występującymi w środowiskach rozproszonych. Przedstawienie mechanizmów zapewniania poufności, integralności, dostępności i rozliczalności w systemach rozproszonych.
C2	Rozwijanie umiejętności analizy bezpieczeństwa systemów rozproszonych poprzez identyfikację podatności, ocenę ryzyka oraz dobór odpowiednich mechanizmów ochrony komunikacji, danych i usług działających w środowiskach rozproszonych.
C3	Zapoznanie studentów z praktycznymi aspektami zabezpieczania systemów rozproszonych, w szczególności usług sieciowych, aplikacji rozproszonych, środowisk chmurowych, kontenerowych oraz mikroserwisowych, z wykorzystaniem współczesnych narzędzi i technologii bezpieczeństwa.
C4	Rozwijanie kompetencji w zakresie projektowania, konfiguracji i oceny bezpiecznych systemów rozproszonych, zarządzania tożsamością i dostępem, monitorowania incydentów bezpieczeństwa oraz stosowania mechanizmów ochrony wykorzystywanych w nowoczesnych środowiskach teleinformatycznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	definiuje podstawowe pojęcia z zakresu systemów rozproszonych oraz ich bezpieczeństwa, w tym system rozproszony, komponent, węzeł, usługę sieciową, komunikację międzyprocesową, architekturę klient-serwer, peer-to-peer, mikroserwisy, system chmurowy oraz środowisko kontenerowe, opisuje zasady współdziałania elementów systemu rozproszonego oraz charakteryzuje podstawowe problemy bezpieczeństwa wynikające z rozproszenia zasobów, danych i usług.	EC2-W1	Kolokwium, Test, Zaliczenie pisemne
W2	charakteryzuje podstawowe zagrożenia występujące w systemach rozproszonych, w tym ataki na komunikację sieciową, przechwytywanie i modyfikację danych, ataki typu Man-in-the-Middle, odmowę usługi, nieuprawniony dostęp do usług, błędy konfiguracji oraz podatności interfejsów API, a także wskazuje mechanizmy ochrony służące zapewnianiu poufności, integralności, dostępności, uwierzytelniania, autoryzacji i rozliczalności.	EC2-W2	Kolokwium, Odpowiedź ustna, Test, Zaliczenie pisemne
W3	opisuje metody zabezpieczania systemów rozproszonych, w tym szyfrowanie komunikacji, stosowanie certyfikatów cyfrowych, mechanizmy kontroli dostępu, zarządzanie tożsamością, ochronę usług sieciowych i interfejsów API, zabezpieczanie środowisk chmurowych, kontenerowych i mikroserwisowych oraz charakteryzuje podstawowe metody monitorowania, wykrywania incydentów, analizy podatności i oceny ryzyka w systemach rozproszonych.	EC2-W1, EC2-W2	Odpowiedź ustna, Test, Zaliczenie pisemne
Umiejętności – Student/ka:			

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U1	analizuje architekturę systemu rozproszonego pod kątem występowania zagrożeń bezpieczeństwa, identyfikuje podatności związane z komunikacją sieciową, współdziałaniem usług, uwierzytelnianiem, autoryzacją oraz wymianą danych między komponentami systemu, a także dobiera mechanizmy ochrony adekwatne do charakteru analizowanego środowiska.	EC2-U3	Kolokwium, Projekt, Rozwiązanie zadania problemowego
U2	konfiguruje wybrane mechanizmy zabezpieczające komunikację, usługi i zasoby w systemach rozproszonych, w tym mechanizmy szyfrowania transmisji, kontroli dostępu, zarządzania tożsamością, ochrony interfejsów API oraz zabezpieczania środowisk chmurowych, kontenerowych i mikroserwisowych.	EC2-U4	Kolokwium, Projekt, Sprawozdanie
U3	interpretuje wyniki monitorowania, testów bezpieczeństwa oraz analizy zdarzeń w systemach rozproszonych, wykrywa nieprawidłowości w konfiguracji i działaniu usług, ocenia skuteczność zastosowanych zabezpieczeń oraz formułuje rekomendacje dotyczące ograniczenia ryzyka i podniesienia poziomu bezpieczeństwa systemu.	EC2-U3, EC2-U4	Prezentacja, Projekt, Rozwiązanie zadania problemowego, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	przestrzega zasad odpowiedzialnego i etycznego postępowania podczas analizy, konfiguracji oraz testowania bezpieczeństwa systemów rozproszonych, uwzględniając możliwe skutki nieprawidłowego wykorzystania narzędzi bezpieczeństwa dla użytkowników, organizacji i infrastruktury teleinformatycznej.	EC2-K4	Odpowiedź ustna, Projekt
K2	ocenia znaczenie aktualizacji wiedzy z zakresu bezpieczeństwa systemów rozproszonych, nowych podatności, zagrożeń, standardów oraz technologii, a także uwzględnia potrzebę stosowania aktualnych zaleceń i dobrych praktyk w projektowaniu oraz zabezpieczaniu środowisk rozproszonych.	EC2-K4	Odpowiedź ustna, Prezentacja, Projekt
K3	współpracuje w zespole podczas rozwiązywania problemów związanych z bezpieczeństwem systemów rozproszonych, komunikuje wyniki analiz i testów bezpieczeństwa w sposób zrozumiały, rzeczowy i zgodny z zasadami odpowiedzialnego raportowania podatności.	EC2-K4	Odpowiedź ustna, Prezentacja, Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do bezpieczeństwa systemów rozproszonych — definicja systemu rozproszonego, cechy systemów rozproszonych, podstawowe architektury, modele komunikacji, wymagania bezpieczeństwa: poufność, integralność, dostępność, uwierzytelnianie, autoryzacja i rozliczalność.	W1, W2, K1	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
2.	Architektury systemów rozproszonych i ich podatności — architektura klient-serwer, peer-to-peer, wielowarstwowa, mikroserwisowa, chmurowa i kontenerowa; zależności między komponentami, punkty krytyczne systemu, ryzyko wynikające z rozproszenia usług, danych i mechanizmów dostępu.	W1, W2, U1	Wykłady, Wykłady synchroniczne
3.	Zagrożenia bezpieczeństwa w systemach rozproszonych — podsłuch i modyfikacja transmisji, ataki Man-in-the-Middle, spoofing, replay attack, przejęcie sesji, ataki DoS/DDoS, nieuprawniony dostęp do usług, błędy konfiguracji oraz podatności interfejsów API.	W2, U1, K1	Wykłady, Wykłady synchroniczne
4.	Bezpieczna komunikacja i ochrona kanałów transmisji — szyfrowanie transmisji, TLS, certyfikaty cyfrowe, wzajemne uwierzytelnianie usług, ochrona komunikacji między komponentami systemu rozproszonego oraz podstawowe zasady zabezpieczania usług sieciowych.	W3, U2	Wykłady, Wykłady synchroniczne
5.	Uwierzytelnianie, autoryzacja i zarządzanie tożsamością — modele kontroli dostępu, role i uprawnienia, tokeny dostępowe, OAuth 2.0, OpenID Connect, Single Sign-On, zarządzanie sesją, zasada najmniejszych uprawnień oraz typowe błędy konfiguracji mechanizmów dostępu.	W3, U2, K1	Wykłady, Wykłady synchroniczne
6.	Bezpieczeństwo usług sieciowych, API i mikroserwisów — zagrożenia dla usług REST, SOAP i GraphQL, kontrola dostępu do API, walidacja danych wejściowych, ograniczanie liczby żądań, ochrona przed nadużyciami, bezpieczeństwo mikroserwisów i komunikacji między usługami.	W2, W3, U1, U2	Wykłady, Wykłady synchroniczne
7.	Bezpieczeństwo środowisk chmurowych i kontenerowych — modele usług chmurowych, współdzielona odpowiedzialność za bezpieczeństwo, izolacja zasobów, zarządzanie sekretami, bezpieczeństwo obrazów kontenerów, podstawowe zagrożenia w środowiskach Docker i Kubernetes.	W3, U2, K2	Wykłady, Wykłady synchroniczne
8.	Monitorowanie, analiza ryzyka i dobre praktyki zabezpieczania systemów rozproszonych — logowanie zdarzeń, analiza logów, wykrywanie incydentów, systemy IDS/IPS i SIEM, identyfikacja podatności, ocena ryzyka, Zero Trust, segmentacja usług, odporność i ciągłość działania systemów rozproszonych.	W2, W3, U3, K2, K3	Wykłady, Wykłady synchroniczne
9.	Analiza architektury przykładowego systemu rozproszonego — identyfikacja komponentów, usług, kanałów komunikacji, punktów dostępu oraz potencjalnych obszarów podatnych na ataki.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
10.	Konfiguracja bezpiecznej komunikacji między usługami — uruchomienie usług sieciowych, konfiguracja szyfrowania transmisji, analiza certyfikatów, sprawdzenie poprawności zabezpieczenia kanału komunikacyjnego.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
11.	Uwierzytelnianie, autoryzacja i ochrona interfejsów API — konfiguracja ról, uprawnień i tokenów dostępowych, analiza błędów kontroli dostępu, testowanie wybranych podatności interfejsów API.	W3, U1, U2, K3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
12.	Bezpieczeństwo kontenerów i usług mikroserwisowych — analiza konfiguracji kontenerów, sprawdzanie uprawnień, ocena izolacji środowisk, identyfikacja podatnych obrazów oraz analiza ryzyka wynikającego z błędnej konfiguracji.	W3, U1, U2, K2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
13.	Monitorowanie i analiza zdarzeń bezpieczeństwa — zbieranie i analiza logów z wielu komponentów systemu rozproszonego, identyfikacja prób ataku, wykrywanie anomalii, interpretacja wyników monitorowania oraz opracowanie wniosków dotyczących bezpieczeństwa systemu.	W3, U3, K3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
14.	Analiza wymagań bezpieczeństwa dla wybranego systemu rozproszonego — określenie celu projektu, identyfikacja aktywów, komponentów, użytkowników, usług, kanałów komunikacji oraz podstawowych wymagań bezpieczeństwa.	W2, U1, K1	Wykłady, Wykłady synchroniczne, Projekty
15.	Modelowanie architektury i identyfikacja zagrożeń — opracowanie schematu architektury systemu, wskazanie punktów krytycznych, analiza możliwych scenariuszy ataku, identyfikacja podatności oraz określenie potencjalnych skutków naruszenia bezpieczeństwa.	W2, U1, K1	Wykłady, Wykłady synchroniczne, Projekty
16.	Dobór mechanizmów zabezpieczających — wybór metod ochrony komunikacji, danych, usług i interfejsów API, dobór mechanizmów uwierzytelniania, autoryzacji, zarządzania tożsamością, kontroli dostępu oraz monitorowania zdarzeń bezpieczeństwa.	W3, U1, U2, K2	Wykłady, Wykłady synchroniczne, Projekty
17.	Konfiguracja lub opracowanie wybranych elementów zabezpieczeń — przygotowanie konfiguracji zabezpieczeń dla usług sieciowych, API, kontenerów, mikroserwisów lub środowiska chmurowego, z uwzględnieniem zasad bezpiecznej konfiguracji i ograniczania uprawnień.	W3, U2, K1, K3	Wykłady, Wykłady synchroniczne, Projekty
18.	Testowanie i ocena skuteczności zabezpieczeń — przeprowadzenie analizy poprawności konfiguracji, testów wybranych mechanizmów ochrony, interpretacja wyników, wskazanie słabych punktów oraz ocena poziomu ryzyka.	W2, W3, U1, U3, K2	Wykłady, Wykłady synchroniczne, Projekty
19.	Opracowanie dokumentacji i prezentacja wyników projektu — przygotowanie raportu zawierającego opis systemu, analizę zagrożeń, zastosowane mechanizmy zabezpieczające, wyniki testów, ocenę ryzyka oraz rekomendacje dotyczące zwiększenia poziomu bezpieczeństwa systemu rozproszonego.	U3, K2, K3	Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć

Wykłady	15
Laboratoria komputerowe	15
Projekty	30
Egzaminy i zaliczenia w sesji	4
Opracowanie sprawozdań z laboratoriów	10
Przygotowanie projektu	10
Przygotowanie się do zajęć	6
Przygotowanie się do kolokwiów i egzaminów	5
Opracowanie dokumentacji technicznej	5
Łączny nakład pracy studenta	**Liczba godzin** 100
Liczba punktów ECTS	**ECTS** 4

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Współczesne metody sztucznej inteligencji

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04180.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 20 • Projekty: 20	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Przedstawienie pojęć związanych z wybranymi technikami i metodami współczesnej sztucznej inteligencji.
C2	Przedstawienie nowoczesnych kierunków rozwoju metod sztucznej inteligencji bazujących na metod głębokich sieci neuronowych.
C3	Omnówienie współczesnych metod bazujących na transformerach.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	zna metody sztucznej inteligencji oraz ich zastosowania w cyberbezpieczeństwie.	EC2-W5	Kolokwium, Projekt
Umiejętności – Student/ka:			
U1	projektuje metody metody sztucznej inteligencji do modelowania cyberzagrożeń.	EC2-U14, EC2-U7	Kolokwium, Projekt
Kompetencji społecznych – Student/ka:			
K1	opracowuje w grupie system stosujący algorytmy sztucznej inteligencji oraz poddaje je krytycznej ocenie w ramach zasad etyki zawodowej oraz odpowiedzialności za skutki społeczne stosowanych rozwiązań informatycznych.	EC2-K3	Kolokwium, Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Optymalizacja struktury neuronowej z zastosowaniem metody gradientu prostego.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
2.	Sieci neuronowe typu feed-forward i algorytm wstecznej propagacji błędu w modelowaniu cyberzagrożeń.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
3.	Splotowe sieci głębokie dla zadań wizyjnych, w tym omówienie architektur z rodziny AlexNet, VGGNet i ResNet.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
4.	Modelowanie języka naturalnego. Omówienie modelu transformera z systemem samouwagi i jego zastosowanie w modelowaniu języka naturalnego.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
5.	Metody fine-tuningowania tansformera, w tym metoda LoRA i destylacja wiedzy.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
6.	Metody kwantyzacji i zabezpieczeń modeli językowych.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Wykłady	15
Laboratoria komputerowe	20
Projekty	20
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	16
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Grafowe bazy danych i ich zastosowania

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.22.04181.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z zagadnieniami dotyczącymi modeli grafowych, sposobów reprezentacji danych powiązanych oraz architektury grafowych systemów bazodanowych.
C2	Rozwijanie umiejętności formułowania kwerend grafowych.
C3	Rozwijanie umiejętności projektowania i implementacji grafowych baz danych oraz wykorzystywania technologii grafowych do analizy danych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	opisuje zaawansowane modele grafowe, mechanizmy zapytań grafowych oraz architekturę grafowych systemów baz danych, wskazując ich zalety, ograniczenia i obszary zastosowań w analizie danych.	EC2-W10	Kolokwium
Umiejętności – Student/ka:			
U1	projektuje i implementuje grafową bazę danych oraz integruje ją z aplikacją lub systemem analitycznym.	EC2-U8	Projekt
U2	analizuje złożone struktury grafowe z wykorzystaniem kwerend i algorytmów grafowych oraz interpretuje otrzymane wyniki w kontekście modelowanej dziedziny.	EC2-U8	Projekt, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	ocenia własną wiedzę i umiejętności w zakresie technologii grafowych, identyfikuje obszary wymagające dalszego rozwoju.	EC2-K1	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Grafowe modele danych i ich miejsce w ekosystemie baz danych.	W1, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
2.	Język zapytań grafowych (Cypher) i operacje na grafach.	W1, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
3.	Projektowanie i implementacja grafowych baz danych.	U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
4.	Algorytmy grafowe i ich zastosowania analityczne.	U2, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
5.	Zastosowania grafowych baz danych w praktyce.	W1, K1	Wykłady, Wykłady synchroniczne, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć

Wykłady	15
Laboratoria komputerowe	15
Projekty	15
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Polityki bezpieczeństwa i zarządzanie ryzykiem

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04167.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty humanistyczne i społeczne

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Nie

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 30, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Przygotowanie studentów do rozumienia i stosowania zasad polityki bezpieczeństwa oraz metod zarządzania ryzykiem w organizacjach publicznych i prywatnych.
C2	Studenci uczą się identyfikować aktywa, zagrożenia i podatności, a następnie przekładać wyniki analizy na konkretne decyzje organizacyjne i zabezpieczenia
C3	Rozwijanie umiejętności tworzenia dokumentacji bezpieczeństwa, formułowania wymagań oraz uzasadniania decyzji zarządczych w oparciu o ryzyko, zgodność i priorytety biznesowe

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Umiejętność projektowania, wdrażania i oceny polityk bezpieczeństwa oraz zarządzanie ryzykiem w organizacji, ze szczególnym uwzględnieniem środowisk złożonych, krytycznych i regulowanych	EC2-W11, EC2-W4	Rozwiązanie zadania problemowego
Umiejętności – Student/ka:			
U1	Definiuje podstawowe pojęcia związane z polityką bezpieczeństwa, ryzykiem, podatnością i podatkiem bezpieczeństwa	EC2-U11, EC2-U14	Rozwiązanie zadania problemowego
U2	Opisuje strukturę polityki bezpieczeństwa oraz jej miejsce w systemie zarządzania organizacją	EC2-U14, EC2-U4	Rozwiązanie zadania problemowego
U3	Przeprowadza podstawową analizę ryzyka z użyciem wybranej metody	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego
U4	Ocenia skuteczność zabezpieczeń i proponuje środki redukcji ryzyka	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego
U5	Rozróżnia ryzyko operacyjne, prawne, technologiczne i reputacyjne	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego
U6	Przygotowuje elementy dokumentacji bezpieczeństwa dla wybranej organizacji	EC2-U11, EC2-U14, EC2-U4	Rozwiązanie zadania problemowego
Kompetencji społecznych – Student/ka:			
K1	Potrafi zaprojektować i zbudować system zabezpieczający infrastrukturę krytyczną i kluczową	EC2-K4	Rozwiązanie zadania problemowego

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Pojęcie bezpieczeństwa informacji, cyberbezpieczeństwa i bezpieczeństwa organizacyjnego	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
2.	Polityka bezpieczeństwa: cele, zakres, zasady, odpowiedzialności	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
3.	Struktura dokumentacji bezpieczeństwa w organizacji	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
4.	Identyfikacja zagrożeń, podatności i skutków	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
5.	Metody analizy i oceny ryzyka	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
6.	Dobór zabezpieczeń organizacyjnych, technicznych i proceduralnych	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
7.	Ciągłość działania, odporność organizacyjna i zarządzanie incydentami	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
8.	Zgodność z normami i regulacjami	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
9.	Polityki bezpieczeństwa w środowiskach IT, OT i infrastruktury krytycznej	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne
10.	Praktyczne studia przypadków i ćwiczenia dokumentacyjne	W1, U1, U2, U3, U4, U5, U6, K1	Wykłady, Wykłady synchroniczne

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	30
Egzaminy i zaliczenia w sesji	2
Konsultacje przedmiotowe	4
Przeprowadzenie badań literaturowych	4
Przygotowanie się do zajęć	4
Przygotowanie prezentacji multimedialnej	6
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Bezpieczeństwo w bazach danych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04182.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z zagrożeniami dla systemów baz danych oraz zasadami projektowania i utrzymywania ich zabezpieczeń, ze szczególnym uwzględnieniem zapewnienia poufności, integralności i dostępności danych, a także identyfikowania i rejestrowania wykonywanych na nich operacji.
C2	Nabycie umiejętności konfigurowania i stosowania mechanizmów uwierzytelniania, autoryzacji, kontroli dostępu, ochrony danych, audytu i monitorowania w systemach Oracle Database i PostgreSQL.
C3	Rozwijanie umiejętności projektowania, implementowania, testowania i oceny bezpiecznych rozwiązań bazodanowych, w tym zabezpieczania kodu i dostępu do danych oraz porównywania mechanizmów bezpieczeństwa dostępnych w różnych systemach zarządzania bazami danych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje zagrożenia dotyczące systemów baz danych, opisuje zasady uwierzytelniania, autoryzacji, kontroli dostępu, szyfrowania, audytu, monitorowania i bezpiecznego programowania baz danych oraz porównuje mechanizmy bezpieczeństwa stosowane w Oracle Database, PostgreSQL i wybranych innych systemach zarządzania bazami danych.	EC2-W2	Kolokwium, Sprawozdanie
Umiejętności – Student/ka:			
U1	analizuje zagrożenia, projektuje, konfiguruje, implementuje i testuje zabezpieczenia systemu baz danych, zarządza kontami, rolami i uprawnieniami, ogranicza dostęp do danych, zabezpiecza kod i komunikację, konfiguruje audyt oraz identyfikuje nieprawidłowości w konfiguracji i działaniu systemu.	EC2-U5, EC2-U8	Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	uzasadnia dobór mechanizmów zabezpieczeń, dokumentuje decyzje dotyczące bezpieczeństwa, ocenia skutki wykrytych podatności i niewłaściwej ochrony danych oraz przestrzega zasad odpowiedzialnego postępowania z danymi i środowiskiem laboratoryjnym.	EC2-K2	Sprawozdanie

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawy bezpieczeństwa baz danych. Klasyfikacja danych oraz wymagania dotyczące ich poufności, integralności i dostępności. Zagrożenia wewnętrzne i zewnętrzne. Identyfikacja elementów systemu baz danych narażonych na atak. Podstawy modelowania zagrożeń i analizy ryzyka. Zasada wielowarstwowej ochrony, najmniejszych uprawnień i rozdzielenia obowiązków. Odpowiedzialność administratora, projektanta, programisty i użytkownika systemu baz danych.	W1, K1	Wykłady, Wykłady synchroniczne, Projekty
2.	Konta użytkowników i uwierzytelnianie. Konta administracyjne, techniczne i aplikacyjne. Polityki haseł, profile użytkowników, blokowanie i wygaszanie kont. Wybrane metody uwierzytelniania w Oracle Database i PostgreSQL. Konfiguracja dostępu klientów do serwera. Ochrona haseł, kluczy, tokenów i innych danych uwierzytelniających wykorzystywanych przez aplikacje do łączenia się z bazą danych. Porównanie z rozwiązaniami stosowanymi w Microsoft SQL Server i MariaDB.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
3.	Role, uprawnienia i zasada najmniejszych uprawnień. Uprawnienia systemowe i obiektowe, role, dziedziczenie uprawnień, własność schematów i obiektów oraz uprawnienia domyślne. Projektowanie macierzy ról i uprawnień. Analiza uprawnień efektywnych, wykrywanie nadmiernych uprawnień oraz ograniczanie zakresu działania kont administracyjnych i aplikacyjnych.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
4.	Ograniczanie dostępu do danych. Wykorzystanie uprawnień, ról, widoków, procedur i funkcji do ograniczania dostępu do danych. Kontrola dostępu na poziomie wiersza, w szczególności Row-Level Security w PostgreSQL oraz wybrane mechanizmy Fine-Grained Access Control lub Virtual Private Database w Oracle Database. Separacja danych należących do różnych użytkowników lub klientów systemu. Podstawy maskowania i anonimizacji danych.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
5.	Bezpieczeństwo aplikacji i kodu bazodanowego. Ataki typu SQL Injection, parametryzacja zapytań, walidacja danych wejściowych oraz ograniczanie uprawnień kont aplikacyjnych. Zagrożenia związane z dynamicznym SQL. Bezpieczne tworzenie i wywoływanie procedur oraz funkcji. Uprawnienia kodu wykonywanego po stronie serwera. Analiza wybranych podatności w kodzie PL/SQL i PL/pgSQL.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
6.	Ochrona danych podczas przesyłania, przechowywania i kopiowania. Zabezpieczanie połączeń klient–serwer z wykorzystaniem TLS. Podstawowe mechanizmy szyfrowania danych, eksportów i kopii zapasowych. Zasady bezpiecznego przechowywania kluczy i danych uwierzytelniających. Maskowanie i anonimizacja danych przekazywanych do środowisk programistycznych i testowych. Porównanie wybranych rozwiązań dostępnych w Oracle Database, PostgreSQL, Microsoft SQL Server i MariaDB.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
7.	Audyt, analiza zdarzeń i bezpieczna konfiguracja systemu baz danych. Rejestrowanie działań administracyjnych, zmian uprawnień, dostępu do danych chronionych i nieudanych prób logowania. Analiza dzienników i identyfikowanie podejrzanych zdarzeń. Ograniczanie dostępu sieciowego i dostępu do narzędzi administracyjnych. Wyłączanie zbędnych kont, usług i funkcji. Identyfikowanie niebezpiecznych ustawień domyślnych oraz przeprowadzanie podstawowego przeglądu konfiguracji bezpieczeństwa.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria komputerowe	15

Projekty	15
Egzaminy i zaliczenia w sesji	4
Opracowanie sprawozdań z laboratoriów	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Podstawy informatyki kwantowej i programowania systemów kwantowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04183.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie z fundamentami fizycznymi i logicznymi obliczeń kwantowych oraz architekturą współczesnych komputerów kwantowych
C2	Wykształcenie umiejętności projektowania, implementacji i uruchamiania obwodów kwantowych w środowisku Qiskit
C3	Przygotowanie do samodzielnej analizy i implementacji algorytmów kwantowych oraz oceny ich wpływu na bezpieczeństwo systemów informatycznych

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	wyjaśnia podstawowe pojęcia informatyki kwantowej, w tym model kubitu, zasady superpozycji, splątania oraz mechanizm pomiaru kwantowego	EC2-W9	Test
W2	opisuje model obliczeń oparty na bramkach kwantowych oraz charakteryzuje uniwersalne zestawy bramek	EC2-W9	Test
W3	klasyfikuje i charakteryzuje najważniejsze algorytmy kwantowe (Deutscha-Jozsy, Grovera, Shora) oraz wskazuje ich przewagę nad rozwiązaniami klasycznymi	EC2-W9	Test
W4	określa wpływ rozwoju komputerów kwantowych na współczesne systemy kryptograficzne i wskazuje założenia kryptografii postkwantowej	EC2-W9	Test
Umiejętności – Student/ka:			
U1	projektuje i implementuje obwody kwantowe realizujące zadane transformacje logiczne z wykorzystaniem biblioteki Qiskit	EC2-U10	Kolokwium, Projekt, Rozwiązanie zadania problemowego
U2	przeprowadza eksperymenty kwantowe na symulatorach i dokonuje krytycznej analizy wyników	EC2-U10	Projekt, Rozwiązanie zadania problemowego
U3	implementuje wybrane algorytmy kwantowe i optymalizuje ich strukturę pod kątem ograniczeń urządzeń klasy NISQ	EC2-U10	Kolokwium, Projekt, Rozwiązanie zadania problemowego
Kompetencji społecznych – Student/ka:			
K1	wykazuje zrozumienie ograniczeń współczesnych technologii kwantowych oraz wykazuje gotowość do krytycznej oceny kierunków ich rozwoju	EC2-K1	Prezentacja, Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do informatyki kwantowej. Historia rozwoju komputerów kwantowych, motywacja biznesowa i naukowa, definicja przewagi kwantowej oraz przegląd aktualnego stanu technologii.	W1	Wykłady, Wykłady synchroniczne
2.	Warsztat programisty kwantowego. Konfiguracja środowiska Python, Jupyter Notebook oraz biblioteki Qiskit. Budowa pierwszego obwodu kwantowego.	U1	Laboratoria komputerowe
3.	Analiza problemu i przygotowanie koncepcji rozwiązania. Wybór tematu projektu, przegląd literatury oraz opracowanie architektury rozwiązania.	W1, W2, W3, W4	Wykłady, Wykłady synchroniczne, Projekty

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Formalizm matematyczny kubitu. Bit klasyczny a kubit, wektory stanu w przestrzeni Hilberta, sfera Blocha oraz fizyczna i logiczna interpretacja pomiaru.	W1	Wykłady, Wykłady synchroniczne
5.	Programowanie stanów podstawowych. Tworzenie kubitów, aplikacja bramek Pauliego i weryfikacja wyników poprzez pomiar.	U1	Laboratoria komputerowe
6.	Projektowanie i implementacja podstawowej funkcjonalności. Budowa obwodów kwantowych oraz przygotowanie środowiska eksperymentalnego.	U1, U3	Projekty
7.	Układy wielokubitowe i splątanie. Rejestry kwantowe, stany splątane, paradoks EPR oraz znaczenie nielokalności w przetwarzaniu informacji.	W1	Wykłady, Wykłady synchroniczne
8.	Manipulacja fazą i superpozycja. Praktyczne zastosowanie bramki Hadamarda, badanie interferencji i analiza rozkładów prawdopodobieństwa.	U1	Laboratoria komputerowe
9.	Rozwój projektu i realizacja eksperymentów. Testowanie algorytmów kwantowych na symulatorach oraz analiza uzyskiwanych wyników.	U2, U3	Projekty
10.	Bramki i obwody kwantowe. Operatory jedno- i wielokubitowe (Hadamard, X, Y, Z, CNOT), uniwersalność bramek oraz zasady konstruowania poprawnych obwodów.	W2	Wykłady, Wykłady synchroniczne
11.	Generowanie splątania. Implementacja stanów Bella, badanie korelacji między kubitami i weryfikacja na symulatorze szumów.	U1, U2	Laboratoria komputerowe
12.	Optymalizacja i walidacja rozwiązania. Analiza ograniczeń urządzeń NISQ, badanie wpływu szumu oraz doskonalenie implementacji.	U2, K1	Projekty
13.	Algorytmiczna przewaga kwantowa. Szczegółowe omówienie algorytmu Deutscha-Jozsy oraz algorytmu przeszukiwania bazy danych Grovera.	W3	Wykłady, Wykłady synchroniczne
14.	Komunikacja kwantowa. Implementacja i analiza protokołu teleportacji kwantowej.	U2	Laboratoria komputerowe
15.	Wykorzystanie symulatora kwantowego, opracowanie dokumentacji technicznej i prezentacja wyników projektu.	K1	Projekty
16.	Kwantowa kryptoanaliza i PQC. Algorytm Shora i jego wpływ na bezpieczeństwo RSA/ECC oraz wprowadzenie do standardów kryptografii postkwantowej (PQC).	W3, W4	Wykłady, Wykłady synchroniczne
17.	Implementacja algorytmów kwantowych. Projektowanie i testowanie algorytmu Deutscha-Jozsy oraz algorytmu Grovera dla prostych problemów wyszukiwania.	U3	Laboratoria komputerowe
18.	Ekosystem systemów kwantowych. Architektury komputerów nadprzewodzących i jonowych (IBM Quantum, Google Quantum AI), ograniczenia ery NISQ i przyszłość technologii.	K1	Wykłady
19.	Kolokwium praktyczne. Samodzielna implementacja wskazanego obwodu lub algorytmu kwantowego wraz z analizą wyników eksperymentu.	U3	Laboratoria komputerowe

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Wykłady	15
Laboratoria komputerowe	15
Projekty	15
Egzaminy i zaliczenia w sesji	4
Przygotowanie się do zajęć	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Zaawansowane modelowanie i analiza systemów informatycznych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04184.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie studentom pogłębionej wiedzy z zakresu modelowania systemów informatycznych z wykorzystaniem notacji UML, DMN i CMMN oraz ich roli w analizie, projektowaniu i dokumentowaniu systemów.
C2	Rozwinięcie umiejętności analizy wymagań, procesów, decyzji i przypadków obsługi złożonych zdarzeń biznesowych oraz odwzorowania ich w modelach strukturalnych, behawioralnych, decyzyjnych i przypadków.
C3	Kształtowanie umiejętności praktycznego wykorzystania narzędzi modelowania do tworzenia spójnej dokumentacji analityczno-projektowej, walidacji modeli oraz komunikacji z interesariuszami projektu.
C4	Zapoznanie studentów z nowoczesnymi podejściami do modelowania i analizy systemów, w tym modelowaniem usług, integracją modeli UML/BPMN/DMN/CMMN, analizą reguł decyzyjnych, dokumentacją lekkiej wagi oraz wykorzystaniem modeli w projektach informatycznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje zaawansowane metody modelowania systemów informatycznych, w tym zastosowanie notacji UML, DMN i CMMN do opisu struktury, zachowania, decyzji oraz przypadków obsługi procesów i zdarzeń.	EC2-W1, EC2-W7	Test
W2	opisuje zasady integracji modeli analitycznych i projektowych, w tym spójność modeli UML z regułami decyzyjnymi DMN, przypadkami CMMN oraz dokumentacją wymagań i architektury systemu.	EC2-W1, EC2-W7	Test
Umiejętności – Student/ka:			
U1	potrafi analizować wymagania i procesy oraz tworzyć modele systemu z wykorzystaniem diagramów UML, tabel decyzyjnych DMN i modeli przypadków CMMN w wybranym narzędziu wspomagającym modelowanie.	EC2-U2, EC2-U3	Projekt, Rozwiązanie zadania problemowego, Sprawozdanie
U2	opracowuje spójną dokumentację analityczno-projektową systemu informatycznego, waliduje modele, identyfikuje niespójności oraz prezentuje przyjęte decyzje modelowe i projektowe.	EC2-U2, EC2-U3	Projekt, Rozwiązanie zadania problemowego, Sprawozdanie
Kompetencji społecznych – Student/ka:			
K1	współpracuje w zespole analityczno-projektowym, komunikuje się z interesariuszami, krytycznie ocenia przyjęte modele i samodzielnie uzupełnia wiedzę na podstawie standardów, dokumentacji i literatury.	EC2-K1	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Rola modeli w analizie i projektowaniu systemów informatycznych; modelowanie jako narzędzie komunikacji, dokumentacji i podejmowania decyzji projektowych.	W1, W2	Wykłady, Wykłady synchroniczne
2.	Zaawansowane modelowanie UML: diagramy przypadków użycia, klas, sekwencji, aktywności, stanów, komponentów i wdrożenia; dobór diagramów do problemu projektowego.	W1, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
3.	Modelowanie wymagań i scenariuszy użycia systemu: aktorzy, przypadki użycia, scenariusze alternatywne, ograniczenia, powiązanie wymagań z modelem systemu.	W1, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
4.	Modelowanie decyzji z wykorzystaniem DMN: wymagania decyzyjne, logika decyzji, tabele decyzyjne, reguły biznesowe, walidacja kompletności i niesprzeczności reguł.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
5.	Modelowanie przypadków i pracy opartej na wiedzy z wykorzystaniem CMMN: przypadki, etapy, zadania, zdarzenia, role oraz kontrola przebiegu pracy nie w pełni ustrukturyzowanej.	W1, W2, U1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
6.	Integracja UML, DMN i CMMN w analizie systemu: spójność modeli, śledzenie wymagań, mapowanie reguł decyzyjnych i przypadków na elementy architektury systemu.	W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
7.	Analiza jakości modeli: kompletność, spójność, czytelność, poziomy abstrakcji, identyfikacja anomalii modelowych oraz typowych błędów w dokumentacji analitycznej.	W2, U1, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
8.	Narzędzia wspomagające modelowanie i analizę systemów: repozytoria modeli, wersjonowanie, eksport dokumentacji, współpraca zespołowa i prezentacja modeli interesariuszom.	U1, U2, K1	Laboratoria komputerowe, Projekty
9.	Nowoczesne zastosowania modeli: dokumentacja lekkiej wagi, modelowanie w projektach zwinnych, modelowanie usług i integracji, przygotowanie modeli do implementacji i testowania.	W1, U1, K1	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe, Projekty
10.	Projekt zespołowy: opracowanie spójnego zestawu modeli UML, DMN i CMMN dla wybranego systemu informatycznego wraz z dokumentacją, walidacją i prezentacją rozwiązania.	U1, U2, K1	Laboratoria komputerowe, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria komputerowe	15
Projekty	15

Egzaminy i zaliczenia w sesji	4
Opracowanie wyników	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Zaawansowane sieci komputerowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Informatyka techniczna i telekomunikacja

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04185.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Laboratoria komputerowe: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Pogłębienie wiedzy z zakresu architektury współczesnych sieci komputerowych oraz zasad projektowania bezpiecznej infrastruktury sieciowej.
C2	Rozwijanie umiejętności zaawansowanej konfiguracji, segmentacji i ochrony sieci w środowisku Cisco.
C3	Nabycie umiejętności monitorowania, diagnozowania i analizowania działania sieci komputerowych z uwzględnieniem aspektów cyberbezpieczeństwa.
C4	Rozwijanie umiejętności projektowania bezpiecznych i skalowalnych rozwiązań sieciowych dla wybranego środowiska organizacyjnego.
C5	Kształtowanie odpowiedzialności za bezpieczeństwo, poprawność konfiguracji i niezawodność infrastruktury sieciowej.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	charakteryzuje architekturę zaawansowanych sieci komputerowych oraz rolę segmentacji, redundancji i mechanizmów bezpieczeństwa w środowisku sieciowym.	EC2-W8	Kolokwium, Test
W2	opisuje mechanizmy ochrony infrastruktury sieciowej, bezpiecznego dostępu administracyjnego, filtrowania ruchu, monitorowania i rejestrowania zdarzeń w środowisku Cisco.	EC2-W8	Kolokwium, Test
Umiejętności – Student/ka:			
U1	projektuje logiczną i funkcjonalną architekturę sieci komputerowej z uwzględnieniem wymagań dostępności, segmentacji i cyberbezpieczeństwa.	EC2-U8	Kolokwium, Projekt
U2	konfiguruje i weryfikuje działanie wybranych zaawansowanych mechanizmów przełączania, routingu, kontroli dostępu i ochrony infrastruktury w środowisku Cisco.	EC2-U8	Kolokwium, Projekt
U3	analizuje ruch sieciowy, logi i informacje diagnostyczne oraz identyfikuje problemy konfiguracyjne, wydajnościowe i bezpieczeństwa w infrastrukturze sieciowej.	EC2-U8	Kolokwium, Projekt
Kompetencji społecznych – Student/ka:			
K1	podejmuje odpowiedzialne działania związane z projektowaniem, konfigurowaniem i zabezpieczaniem infrastruktury sieciowej oraz systematycznie aktualizuje własne kompetencje w zakresie nowoczesnych technologii sieciowych i cyberbezpieczeństwa.	EC2-K2	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Architektura nowoczesnych sieci komputerowych: sieci kampusowe, sieci oddziałowe, segmentacja funkcjonalna, wymagania dostępności, skalowalności i bezpieczeństwa.	W1	Wykłady, Wykłady synchroniczne
2.	Zaawansowane przełączanie i segmentacja ruchu: logiczny podział sieci, separacja ruchu, redundancja warstwy drugiej oraz wybrane mechanizmy ochrony warstwy drugiej.	W1, W2, U2	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
3.	Zaawansowany routing i organizacja komunikacji między segmentami: projektowanie przepływu ruchu, niezawodność, ciągłość działania usług oraz diagnostyka problemów routingu.	W1, U1, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
4.	Bezpieczna konfiguracja urządzeń Cisco: bezpieczny dostęp administracyjny, twarda konfiguracja urządzeń, zarządzanie uprawnieniami i podstawy ochrony płaszczyzny zarządzania.	W2, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
5.	Mechanizmy kontroli i filtrowania ruchu: polityki dostępu, separacja stref komunikacji, ograniczanie ruchu nieautoryzowanego oraz wybrane mechanizmy translacji adresów.	W2, U1, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
6.	Monitorowanie i diagnostyka sieci: rejestrowanie zdarzeń, analiza działania urządzeń, interpretacja logów i informacji diagnostycznych, wykrywanie błędów konfiguracyjnych i anomalii ruchu.	W2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
7.	Bezpieczny dostęp do usług i zasobów sieciowych: kontrola dostępu do sieci przewodowej i bezprzewodowej, bezpieczny dostęp zdalny oraz podstawowe mechanizmy ochrony usług sieciowych.	W1, W2, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
8.	Podstawy automatyzacji i programowalności sieci: powtarzalność konfiguracji, standaryzacja zarządzania, ograniczanie błędów administracyjnych oraz znaczenie automatyzacji dla bezpieczeństwa sieci.	W2, U2, U3	Wykłady, Wykłady synchroniczne, Laboratoria komputerowe
9.	Projekt bezpiecznej sieci komputerowej w środowisku Cisco: analiza wymagań, dobór architektury, segmentacji, polityk bezpieczeństwa, dokumentacji technicznej i sposobu zarządzania infrastrukturą.	W1, W2, U1, U2, U3, K1	Wykłady synchroniczne, Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Laboratoria komputerowe	15
Projekty	15
Egzaminy i zaliczenia w sesji	4

Przygotowanie sprawozdań, raportów, projektów, prezentacji	1
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Wizja komputerowa w systemach inteligentnych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.04186.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Wykłady: 15, w tym zajęcia zdalne: ◦ Wykłady synchroniczne: 15 • Projekty: 15	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z rolą wizji komputerowej jako układu sensorycznego systemów inteligentnych, z modelem formowania obrazu cyfrowego oraz z etapami procesu przetwarzania danych wizyjnych.
C2	Przekazanie wiedzy z zakresu klasycznej ekstrakcji cech i klasyfikacji obrazów oraz wprowadzenie do konwolucyjnych sieci neuronowych (CNN) i uczenia transferowego.
C3	Przekazanie wiedzy o wizyjnych mechanizmach uwierzytelniania i nadzoru (biometria twarzy, detekcja i śledzenie obiektów, wykrywanie zdarzeń nietypowych) w kontekście systemów bezpieczeństwa.
C4	Zapoznanie studentów z zagrożeniami bezpieczeństwa systemów wizyjnych (ataki adwersarialne, obrazy manipulowane metodami generatywnymi), a także z podstawowymi metodami ich wykrywania.
C5	Rozwinięcie kompetencji w zakresie projektowania, implementacji i dokumentowania inteligentnego systemu wizyjnego w pracy zespołowej, z uwzględnieniem zasad etyki oraz ochrony danych osobowych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	definiuje proces powstawania obrazu cyfrowego, opisuje reprezentację obrazu w wybranych przestrzeniach barw oraz charakteryzuje etapy procesu przetwarzania danych wizyjnych w systemach inteligentnych.	EC2-W10	Odpowiedź ustna, Prezentacja, Projekt, Sprawozdanie, Zaliczenie pisemne
W2	charakteryzuje klasyczne oraz oparte na sieciach CNN metody klasyfikacji i detekcji obiektów, a także opisuje zagrożenia bezpieczeństwa systemów wizyjnych (ataki adwersarialne, manipulacja obrazów metodami generatywnymi) oraz podstawowe mechanizmy prewencyjne.	EC2-W10	Odpowiedź ustna, Prezentacja, Projekt, Sprawozdanie, Zaliczenie pisemne
Umiejętności – Student/ka:			
U1	implementuje algorytmy przetwarzania i analizy obrazu oraz algorytmy klasyfikatorów i detektorów obiektów z wykorzystaniem biblioteki OpenCV, sieci CNN i uczenia transferowego w języku Python.	EC2-U7, EC2-U9	Odpowiedź ustna, Prezentacja, Projekt, Sprawozdanie, Zaliczenie pisemne
U2	projektuje, testuje i dokumentuje komponenty inteligentnego systemu wizyjnego, dobiera metody oceny jego odporności na zagrożenia oraz uwzględnia wymagania ochrony danych osobowych.	EC2-U7, EC2-U9	Odpowiedź ustna, Prezentacja, Projekt, Sprawozdanie, Zaliczenie pisemne
Kompetencji społecznych – Student/ka:			
K1	współpracuje w zespole projektowym, przestrzega zasad etyki zawodowej oraz regulacji dotyczących ochrony danych osobowych i przyjmuje odpowiedzialność za jakość realizowanych zadań.	EC2-K1	Prezentacja, Projekt, Sprawozdanie

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wizja komputerowa w systemach inteligentnych — architektura systemu, etapy procesu analizy obrazu, reprezentacje obrazu cyfrowego, przestrzenie barw. Zastosowania w obszarze cyberbezpieczeństwa.	W1	Wykłady, Wykłady synchroniczne
2.	Podstawe metody analizy danych wizyjnych — filtracja, detekcja krawędzi, ekstrakcja cech.	W1, U1	Wykłady, Wykłady synchroniczne, Projekty
3.	Klasyczne metody klasyfikacji obrazów — wyznaczanie wektorów cech, klasyfikatory k-NN i SVM, podstawy oceny skuteczności modeli (macierz pomyłek, dokładność, precyzja, czułość).	W2, U1	Wykłady, Wykłady synchroniczne, Projekty
4.	Konwolucyjne sieci neuronowe (CNN) i uczenie transferowe — architektura sieci, douczanie sieci wstępnie wytrenowanych, trening nowych modeli.	W2, U1	Wykłady, Wykłady synchroniczne, Projekty
5.	Biometria wizyjna — detekcja i rozpoznawanie twarzy, wizyjne uwierzytelnianie i kontrola dostępu; ograniczenia metod oraz ochrona danych osobowych.	W2, U2	Wykłady, Wykłady synchroniczne, Projekty
6.	Bezpieczeństwo modeli wizyjnych — ataki z użyciem celowo zaburzonych danych wejściowych (ataki adwersarialne; metody FGSM, PGD — ujęcie koncepcyjne), podstawowe mechanizmy prewencyjne.	W2, U2	Wykłady, Wykłady synchroniczne, Projekty
7.	Wykrywanie manipulacji obrazu — analiza autentyczności obrazów, artefakty obrazów sztucznie wygenerowanych, wykrywanie obrazów zmanipulowanych metodami generatywnymi.	W2, U2	Wykłady, Wykłady synchroniczne, Projekty
8.	Inteligentny nadzór wizyjny — detekcja i śledzenie obiektów, wykrywanie zdarzeń nietypowych; przegląd zastosowań oraz aspekty etyczne i prawne.	W1, W2	Wykłady, Wykłady synchroniczne, Projekty
9.	Projektowanie, implementacja, testowanie i dokumentowanie systemów wizyjnych — praca zespołowa nad rozwiązaniem problemu inżynierskiego.	U1, U2, K1	Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykłady	15
Projekty	15
Egzaminy i zaliczenia w sesji	3
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	4
Przygotowanie się do kolokwiów i egzaminów	6
Przygotowanie sprawozdań, raportów, projektów, prezentacji	7

Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Kształcenie projektowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.02732.26

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Projekty: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekazanie studentom wiedzy z zakresu prowadzenia projektów informatycznych zorientowanych na analizę, modelowanie, dokumentowanie i weryfikację rozwiązań systemowych w kontekście potrzeb organizacji i interesariuszy.
C2	Rozwinięcie umiejętności zaawansowanej analizy systemu, obejmującej identyfikację interesariuszy, analizę problemu, określenie zakresu, model as-is/to-be, wymagania funkcjonalne i niefunkcjonalne oraz zależności między procesami i komponentami systemu.
C3	Kształtowanie umiejętności wykorzystania notacji BPMN oraz wybranych technik zaawansowanego modelowania do opisu procesów biznesowych, przepływów informacji, decyzji, przypadków użycia, architektury systemu i integracji z otoczeniem.
C4	Przygotowanie studentów do zespołowej realizacji projektu analityczno-projektowego, obejmującego planowanie prac, komunikację z interesariuszami, walidację modeli, przygotowanie dokumentacji oraz prezentację i obronę przyjętych rozwiązań.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	opisuje zasady prowadzenia projektu analityczno-projektowego, w tym etapy pracy projektowej, role w zespole, współpracę z interesariuszami, dokumentowanie wymagań oraz specyfikę zaawansowanej analizy systemu.	EC2-W11	Odpowiedź ustna, Projekt
W2	charakteryzuje metody modelowania procesów i systemów z wykorzystaniem notacji BPMN oraz wybranych technik zaawansowanego modelowania, w tym modelowania wymagań, przypadków użycia, decyzji, danych, komponentów i integracji systemu.	EC2-W11	Odpowiedź ustna, Projekt
Umiejętności – Student/ka:			
U1	potrafi przeprowadzić zaawansowaną analizę systemu, obejmującą identyfikację problemu, interesariuszy, zakresu, wymagań, ryzyk, procesów as-is/to-be oraz ograniczeń technicznych i organizacyjnych.	EC2-U10, EC2-U2, EC2-U3	Prezentacja, Projekt
U2	potrafi opracować spójny zestaw modeli i dokumentacji projektowej z wykorzystaniem BPMN oraz wybranych notacji modelowania systemów, a także zweryfikować, zaprezentować i uzasadnić przyjęte rozwiązania.	EC2-U10, EC2-U2, EC2-U3	Prezentacja, Projekt
Kompetencji społecznych – Student/ka:			
K1	współpracuje w zespole projektowym, komunikuje się z interesariuszami, odpowiedzialnie planuje i dokumentuje pracę oraz krytycznie ocenia modele, wymagania i decyzje projektowe.	EC2-K1, EC2-K2, EC2-K5	Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Organizacja projektu analityczno-projektowego: cel projektu, zakres, role w zespole, interesariusze, harmonogram, sposób dokumentowania pracy oraz zasady komunikacji projektowej.	W1, W2, K1	Projekty
2.	Zaawansowana analiza systemu: identyfikacja problemu, analiza otoczenia systemu, określenie granic systemu, ograniczeń technicznych i organizacyjnych oraz kluczowych wymagań biznesowych i systemowych.	W1, U1	Projekty
3.	Analiza i modelowanie procesów biznesowych z wykorzystaniem BPMN: modele as-is i to-be, uczestnicy procesu, zdarzenia, zadania, bramki decyzyjne, przepływy oraz identyfikacja miejsc wymagających usprawnienia.	W2, U1, U2	Projekty
4.	Modelowanie wymagań i zachowania systemu: przypadki użycia, scenariusze, diagramy aktywności, przepływy informacji oraz powiązanie wymagań z procesami biznesowymi i funkcjami systemu.	W2, U1, U2	Projekty
5.	Zaawansowane modelowanie struktury i integracji systemu: model danych, komponenty, interfejsy, zależności między modułami, integracja z innymi systemami oraz analiza spójności przyjętej architektury.	W2, U2	Projekty
6.	Analiza decyzji projektowych, ryzyka i jakości rozwiązania: identyfikacja ryzyk, ograniczeń, wariantów rozwiązania, kryteriów wyboru oraz ocena wpływu decyzji projektowych na funkcjonowanie systemu	W1, U1, U2, K1	Projekty
7.	Opracowanie dokumentacji analityczno-projektowej: opis wymagań, modele BPMN i modele systemowe, uzasadnienie przyjętych rozwiązań, walidacja modeli oraz przygotowanie spójnego raportu projektowego.	U1, U2, K1	Projekty
8.	Projekt zespołowy: wykonanie pełnej analizy systemu, przygotowanie modeli procesów i systemu, opracowanie dokumentacji, prezentacja rozwiązania oraz odpowiedź ustna dotycząca przyjętych decyzji projektowych.	U1, U2, K1	Projekty

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Projekty	30
Egzaminy i zaliczenia w sesji	2
Opracowanie wyników	8

Przygotowanie projektu	10
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Seminarium dyplomowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.01917.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Seminaria: 30	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z wymaganiami merytorycznymi i formalnymi w zakresie przygotowywania i obrony pracy inżynierskiej, w tym zasadami ochrony własności intelektualnej i prawa autorskiego.
C2	Przygotowanie studentów do syntetycznej i klarownej prezentacji wyników swojej pracy oraz aktywnego udziału w merytorycznej dyskusji na jej temat.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	rozróżnia teorie i koncepcje z zakresu problematyki badań prowadzonych na potrzeby pracy dyplomowej oraz zasady działania organizacji, w których prowadzi badania, w tym zasady etyczne i bezpieczeństwa informacji.	EC2-W11, EC2-W12	Prezentacja
Umiejętności – Student/ka:			
U1	pozyskuje z literatury, baz danych oraz innych źródeł informacje niezbędne do przygotowania prezentacji związanej z planowaną pracą dyplomową, a następnie dokonuje selekcji i krytycznej oceny ich wartości.	EC2-U1, EC2-U13	Prezentacja
U2	redaguje tekst techniczny zgodnie z wymogami edytorskimi i językowymi obowiązującymi na kierunku.	EC2-U1, EC2-U14	Prezentacja
U3	przygotowuje i przedstawia prezentację dotyczącą pracy dyplomowej, uwzględniającą elementy popularyzujące badaną tematykę oraz prowadzi dyskusję po prezentacji, występując w roli eksperta	EC2-U1, EC2-U13, EC2-U14	Prezentacja
Kompetencji społecznych – Student/ka:			
K1	analizuje i krytycznie ocenia postęp prac oraz jest gotowy do samodzielnego oraz zespołowego projektowania i prowadzenia badań naukowych z wykorzystaniem różnorodnych źródeł informacji.	EC2-K1, EC2-K5	Prezentacja

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wymagania formalne pracy dyplomowej: struktura, elementy obowiązkowe, kryteria oceny promotora i recenzenta.	U1	Seminaria
2.	Prawo autorskie, etyka zawodowa i procedura antyplagiatowa: zasady cytowania, tworzenie referencji, obsługa systemu antyplagiatowego.	W1	Seminaria
3.	Temat, cel i zakres pracy dyplomowej. Praca nad tekstem technicznym zgodnie z obowiązującymi na kierunku wymogami edytorskimi i językowymi.	W1, U1, U2, K1	Seminaria
4.	Prezentacje indywidualne wyników pracy dyplomowej na forum grupy i dyskusje na ich temat.	W1, U1, U2, U3, K1	Seminaria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Seminaria	30

Egzaminy i zaliczenia w sesji	2
Przygotowanie sprawozdań, raportów, projektów, prezentacji	18
Łączny nakład pracy studenta	**Liczba godzin** 50
Liczba punktów ECTS	**ECTS** 2

* godzina (aktywności studenta) oznacza 45 minut

Politechnika Krakowska
im. Tadeusza Kościuszki

Przygotowanie pracy dyplomowej

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
Informatyka i cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Inżynierii Elektrycznej i Komputerowej

Poziom studiów
II stopnia (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
ogólnoakademicki

Dyscypliny
Automatyka, elektronika, elektrotechnika i technologie kosmiczne

Cykl dydaktyczny
2026/27

Kod zajęć
WEECS.24.01838.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Zajęcia powiązane z badaniami prowadzonymi w uczelni
Tak

Zajęcia kształtujące umiejętności praktyczne
Nie

Okres	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie **Forma prowadzenia i godziny zajęć** • Seminaria: 12	18

Cele kształcenia dla zajęć

Kod	Cel
C1	Przygotowanie studenta do realizacji pracy dyplomowej magisterskiej będącej samodzielnym opracowaniem zagadnienia naukowego lub naukowo-inżynierskiego.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
W1	rozróżnia metody i techniki badawcze stosowane w ramach realizowanego badania naukowego oraz metody zachowania bezpieczeństwa, w tym bezpieczeństwa wymiany informacji.	EC2-W11, EC2-W12	Praca dyplomowa
Umiejętności – Student/ka:			
U1	formułuje problem naukowy lub naukowo-inżynierski będący podstawą pracy dyplomowej magisterskiej.	EC2-U1, EC2-U13	Praca dyplomowa
U2	dobiera narzędzia i metody niezbędne do osiągnięcia celu pracy dyplomowej.	EC2-U1, EC2-U13, EC2-U14	Praca dyplomowa
U3	rozwiązuje problem naukowy lub naukowo-inżynierski, w szczególności poprzez przeprowadzenie badań lub wykonanie obliczeń projektowych lub analizę problemu inżynierskiego. Dokonuje analizy i interpretacji uzyskanych wyników oraz opracowuje pracę spełniającą wymagania stawiane pracy dyplomowej na poziomie 6 PRK.	EC2-U1, EC2-U13, EC2-U14	Praca dyplomowa
Kompetencji społecznych – Student/ka:			
K1	organizuje własną pracę w ramach realizacji pracy dyplomowej, a jej postępy konsultuje na bieżąco z promotorem, uwzględniając uwagi wynikające z dyskusji nad otrzymanymi wynikami.	EC2-K1, EC2-K5	Praca dyplomowa
K2	dostrzega potrzebę ciągłego doskonalenia zawodowego oraz aktualizuje wiedzę w obszarze związanym z tematyką pracy dyplomowej.	EC2-K1, EC2-K5	Praca dyplomowa

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Indywidualny zakres zajęć uzależniony od tematu i charakteru pracy inżynierskiej.	W1, U1, U2, U3, K1, K2	Seminaria

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Seminaria	12
Egzaminy i zaliczenia w sesji	2
Opracowanie wyników	211
Przygotowanie pracy dyplomowej	160
Przeprowadzenie badań literaturowych	35

Zbieranie informacji do pracy dyplomowej	30
Łączny nakład pracy studenta	**Liczba godzin** 450
Liczba punktów ECTS	**ECTS** 18

* godzina (aktywności studenta) oznacza 45 minut