

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo aplikacji webowych, PG_00155306						
Kierunek studiów	Informatyka (P)						
Data rozpoczęcia studiów	październik 2025 r.		Rok akademicki realizacji przedmiotu		2026/2027		
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z praktycznym przygotowaniem zawodowym - profil praktyczny		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski		
Semestr studiów	4		Liczba punktów ECTS		2.0		
Profil kształcenia	praktyczny		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Rektor -> Wydział Matematyki, Fizyki i Informatyki -> Instytut Informatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Jakub Neumann				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	15.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30		0.0		20.0	50
Cel przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z zagadnieniami związanymi z bezpieczeństwem aplikacji internetowych w tym sposobów prawidłowego projektowania aplikacji pod kątem bezpieczeństwa, wykorzystania dedykowanych/specjalistycznych protokołów oraz przeciwdziałania popularnym atakom. Szczególny nacisk położony jest na protokoły OAuth2/OpenIDConnect i zagadnienia bezpiecznego udostępniania API						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[INFL3_U06] potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami szyfrowania danych	potrafi bezpiecznie udostępniać API zgodnie z OAuth2 flows/ grants, posługiwać się odpowiednimi bibliotekami do obsługi OAuth2, zarządzać serwerem autoryzacyjnym Keycloak	[SU2] prezentacja/projekt/referat/ raport [SU4] test/egzamin - ustny lub pisemny
	[INFL3_U03] potrafi pracować w zespole informatyków, zarządzać swoim czasem oraz podejmować zobowiązania i dotrzymywać terminy, porozumiewać się przy użyciu różnych technik w środowisku zawodowym w tym z wykorzystaniem dedykowanych narzędzi	potrafi dotrzymywać zobowiązań, także czasowych wynikających z realizacji zadań projektowych, współpracować w grupie realizującej podobne zadania	[SU2] prezentacja/projekt/referat/ raport [SU4] test/egzamin - ustny lub pisemny
	[INFL3_W07] ma wiedzę w zakresie projektowania, wytwarzania, testowania, wdrażania i utrzymania aplikacji webowych oraz ich bezpieczeństwa	ma wiedzę związana z zagadnieniami bezpieczeństwa aplikacji webowych, przeciwdziałania popularnym atakom, w szczególności zna zasady związane z flows/grants protokołów OAuth2/ OpenIDConnect	[SW4] test/egzamin - ustny lub pisemny [SW2] prezentacja/projekt/referat/ raport
	[INFL3_K02] potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania	potrafi precyzyjnie formułować pytania związane z bezpieczeństwem aplikacji webowych i protokołami OAuth2/ OpenIDConnect, w szczególności posługiwać się pojęciami takimi jak Resource Server, Authorization Server, Resource Owner, Client, User Agent	[SK2] prezentacja/projekt/referat/ raport [SK4] test/egzamin - ustny lub pisemny
Treści przedmiotu	• Uwierzytelnianie, autoryzacja, typowe zagadnienia bezpieczeństwa systemów informatycznych • Bezpieczeństwo protokołu HTTP, rola protokołu TLS, zabezpieczanie udostępnianego HTTP API • HTTP Basic Authorisation • protokoły OAuth2, Authorization Code Flow/Grant, Client Credential Flow/Grant, OpenID Connect • konfiguracja usług uwierzytelniania i autoryzacji usług na przykładzie serwisu Auth0/Okta • lokalny serwis usług uwierzytelniani i autoryzacji na przykładzie serwera Keycloak		
Wymagania wstępne i dodatkowe	Zaliczony przedmiot "Protokoły sieci web"		
Sposoby i kryteria oceniania osiąganych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	kolokwium	51.0%	60.0%
	projekty	51.0%	40.0%
Zalecana lista lektur	Podstawowa lista lektur	Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, aut. Andrew Hoffman, ISBN 9788328370050	
	Uzupełniająca lista lektur	Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona, aut.Malcolm McDonald, 9788328378032	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		