



Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów i sieci, PG_00047746						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	październik 2023 r.	Rok akademicki realizacji przedmiotu			2024/2025		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	niestacjonarne	Sposób realizacji			na uczelni		
Rok studiów	2	Język wykładowy			polski		
Semestr studiów	3	Liczba punktów ECTS			4.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Jacek Rak					
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Jacek Rak					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	12.0	0.0	0.0	15.0	0.0	27
	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	27	10.0		63.0		100
Cel przedmiotu	Poznanie zagrożeń dla sieci podłączonych do Internetu, rodzajów naruszeń bezpieczeństwa systemów komputerowych, metod zabezpieczania się przed atakami, zrozumienie roli polityki bezpieczeństwa oraz metod zarządzania bezpieczeństwem systemów informatycznych						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_U08] potrafi przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich oraz ich rozwiązywaniu: – wykorzystać metody analityczne, symulacyjne i eksperymentalne, – dostrzegać ich aspekty systemowe i pozatechniczne, – dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań i podejmowanych działań inżynierskich	Student potrafi zaproponować rozwiązanie bezpieczeństwa biorące pod uwagę zagrożenia środowiska systemów i sieci.	[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania
	[K7_U09] potrafi dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i ocenić te rozwiązania, a także wykorzystać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem zaawansowanych urządzeń, obiektów i systemów technicznych typowych dla kierunku studiów	Student potrafi zaproponować rozwiązanie bezpieczeństwa biorące pod uwagę czynniki charakteryzujące środowisko systemów i sieci.	[SU1] Ocena realizacji zadania
	[K7_W09] zna i rozumie w pogłębionym stopniu ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z nadaną kwalifikacją, w tym zasady ochrony własności przemysłowej i prawa autorskiego	Student rozumie znaczenia polityki bezpieczeństwa jako fundamentu bezpieczeństwa całego systemu.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
[K7_W08] zna i rozumie w pogłębionym stopniu fundamentalne dylematy współczesnej cywilizacji, główne trendy rozwojowe dyscyplin naukowych istotnych dla kierunku kształcenia	Student zna zabezpieczenia systemów informatycznych, wybranych algorytmów szyfrowania, standardów bezpieczeństwa systemów, infrastruktury klucza publicznego.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym	
Treści przedmiotu	Zagrożenia bezpieczeństwa systemów sieciowych. Klasy zagrożeń bezpieczeństwa systemów sieciowych. Kategorie i techniki ataków. Typy zapór sieciowych. Konfiguracje zapór sieciowych. Systemy kontroli dostępu. Systemy wykrywania intruzów. Wirtualne sieci prywatne VPN - klasyfikacja. Protokoły VPN - L2. Protokoły VPN - L3-5. Polityka bezpieczeństwa. Utrzymywanie poziomu bezpieczeństwa. Ocena poziomu bezpieczeństwa. Audyt		
Wymagania wstępne i dodatkowe	Nie ma wymagań		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Projekt	50.0%	50.0%
	Egzamin pisemny	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	J. Stokłosa, T. Biłski, T. Pankowski: "Bezpieczeństwo danych w systemach informatycznych", PWN, Warszawa Poznań, 2001 A. Białas: "Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie", WNT, Warszawa 2007 K. Liderman: "Podręcznik administratora bezpieczeństwa teleinformatycznego", Mikom, Warszawa 2003 K. Liderman: "Analiza ryzyka i ochrona informacji w systemach komputerowych", PWN, Warszawa 2008	
	Uzupełniająca lista lektur	Nie ma wymagań	
	Adresy eZasobów	Adresy na platformie eNauczanie:	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		