



Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo, PG_00062743						
Kierunek studiów	Technologie Przemysłu 5.0						
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu			2028/2029		
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć			Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć z obszarów nauk humanistycznych lub nauk społecznych		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	3	Język wykładowy			polski		
Semestr studiów	6	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Jacek Rak					
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	0.0	0.0	15.0	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	2.0	18.0	50		
Cel przedmiotu	Celem jest zapoznanie studentów z podstawami cyberbezpieczeństwa. W ramach przedmiotu przewidziane jest omówienie m.in. następujących zagadnień: zagrożenia dla bezpieczeństwa w tym w szczególności w kontekście korzystania z zasobów Internetu; rodzaje ataków: poznanie/modyfikacja treści, podszywanie, ataki celowane i niecelowane, malware, sieci botnet; analiza atrybutów bezpieczeństwa takich jak poufność, autentyczność, dostępność, integralność danych, czy niezaprzeczalność oraz mechanizmów ich zapewniania; polityka bezpieczeństwa; dobre praktyki bezpieczeństwa.						
Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu			Sposób weryfikacji i oceny efektu		
	[K6_W04] wykazuje się wiedzę niezbędną do rozumienia pozatechnicznych (prawnych, ekonomicznych, etycznych, środowiskowych) uwarunkowań działalności inżynierskiej w zakresie bezpośrednio lub pośrednio związanym z rewolucją przemysłową	Student rozumie zagrożenia bezpieczeństwa, charakteryzuje główne rodzaje ataków, zna środki bezpieczeństwa właściwe dla systemów informatycznych.			[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		
	[K6_U04] potrafi dostrzec i uwzględnić aspekty pozatechniczne (prawne, ekonomiczne, etyczne, środowiskowe, czynnik ludzki i inne) problemów i zadań inżynierskich oraz tworzyć rozwiązania je uwzględniające	Student potrafi zaproponować rozwiązanie bezpieczeństwa biorące pod uwagę zagrożenia charakteryzujące środowisko systemów i sieci.			[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania		
	[K6_W71] ma wiedzę ogólną z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych	Student rozumie znaczenie polityki bezpieczeństwa jako fundamentu bezpieczeństwa całego systemu.			[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		
[K6_U71] potrafi zastosować wiedzę z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych do rozwiązywania problemów w środowisku społecznym	Student potrafi zaproponować rozwiązanie bezpieczeństwa biorące pod uwagę czynniki charakteryzujące środowisko systemów i sieci.			[SU1] Ocena realizacji zadania			

Treści przedmiotu	Treści przedmiotu - wykład 1. Zagrożenia bezpieczeństwa systemów sieciowych 2. Atrybuty bezpieczeństwa 3. Kategorie i techniki ataków 4. Oprogramowanie malware 5. Sieci botnet 6. Typy zapór sieciowych 7. Konfiguracje zapór sieciowych 8. Systemy kontroli dostępu 9. Systemy wykrywania intruzów 10. Wirtualne sieci prywatne (VPN) 11. Polityka bezpieczeństwa 12. Dobre praktyki bezpieczeństwa 13. Utrzymywanie poziomu bezpieczeństwa 14. Ocena poziomu bezpieczeństwa 15. Audyt		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	seminarium	50.0%	50.0%
	zaliczenie	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	1. Materiały wykładowe  2. A. Białas: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT (2007)  3. S. Enoka: Cyberbezpieczeństwo w małych sieciach. Helion (2024)	
	Uzupełniająca lista lektur	J. Rak: Resilient Routing in Communication Networks A Systems Perspective, 2 <sup>nd</sup> Edition. Springer (2024) K. Liderman: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN (2008)  K. Liderman: Podręcznik administratora bezpieczeństwa teleinformatycznego. Mikom (2003)	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	W ramach seminarium studenci w ramach grup 2-osobowych przygotowują i przedstawiają opracowanie własne wybranego zagadnienia z obszaru cyberbezpieczeństwa.		
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.