

Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM, PG_00061382						
Kierunek studiów	Zarządzanie inżynierskie						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu		2026/2027		
Poziom kształcenia	I stopnia - inżynierskie		Grupa zajęć		Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	3		Język wykładowy		polski		
Semestr studiów	6		Liczba punktów ECTS		3.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Zarządzania i Ekonomii -> Katedra Informatyki W Zarządzaniu						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr hab. inż. Rafał Leszczyna				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć i metody nauczania	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		6.0		39.0	75
Cel przedmiotu	Analizuje i ocenia krytycznie zagrożenia cyberbezpieczeństwa zasobów informatycznych przedsiębiorstwa projektując odpowiednie środki ochrony						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K6_W03] identyfikuje wiarygodne źródła informacji istotne dla analizowanych zagadnień		analizuje przedsiębiorstwo i jego zasoby informatyczne identyfikując zagrożenia cyberbezpieczeństwa		[SW1] Ocena wiedzy faktograficznej		
	[K6_U07] stosuje technologie informatyczne w celu usprawnienia krytycznej analizy i oceny danych i procesów zarządzania		ocenia krytycznie problemy zagrożeń cyberbezpieczeństwa w przedsiębiorstwie i definiuje odpowiednie środki ochrony		[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu		
Treści przedmiotu	Podstawowe pojęcia i koncepcje cyberbezpieczeństwa Używalne cyberbezpieczeństwo Proces zarządzania cyberbezpieczeństwem Zarządzanie ryzykiem cyberbezpieczeństwa Zagrożenia cyberbezpieczeństwa Wybrane standardy i wytyczne dotyczące cyberbezpieczeństwa Zabezpieczenia						
Wymagania wstępne i dodatkowe							
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)		Próg zaliczeniowy		Składowa oceny końcowej		
	Sprawdzian wiedzy		60.0%		45.0%		
	Aktywne uczestniczenie w wykładzie		60.0%		5.0%		
	Ćwiczenia laboratoryjne		60.0%		50.0%		

Zalecana lista lektur	Podstawowa lista lektur	ISO/IEC 27001:2017 NIST SP 800-53 Revision 5 Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014 Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011
	Uzupełniająca lista lektur	Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 ISO/IEC 15408 (Common Criteria) Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017
	Adresy eZasobów	Adresy na platformie eNauczanie:
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Przeprowadź analizę przedsiębiorstwa. Zidentyfikuj i opisz jego cyberzasoby Zidentyfikuj niezależne listy zagrożeń cyberbezpieczeństwa i opracuj własną listę cyberzagrożeń Oszacuj ryzyko cyberbezpieczeństwa Wyjaśnij systematyczne podejście do zarządzania cyberbezpieczeństwem w przedsiębiorstwie Wybierz standard cyberbezpieczeństwa, uzasadnij swój wybór Podaj przykład naruszenia integralności cyberzasobu Podaj przykład zabezpieczenia służącego zmniejszeniu ryzyko skopiowania danych księgowych przez nieuprawnionych użytkowników Podaj i wyjaśnij wzór na ryzyko cyberbezpieczeństwa Wskaż i wyjaśnij najczęstsze strategie postępowania z zagrożeniami związanymi z cyberbezpieczeństwem Opisz podstawowe cechy kontroli dostępu	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.