



Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM , PG_00056590						
Kierunek studiów	Zarządzanie inżynierskie						
Data rozpoczęcia studiów	październik 2022 r.		Rok akademicki realizacji przedmiotu		2025/2026		
Poziom kształcenia	I stopnia - inżynierskie		Grupa zajęć				
Forma studiów	stacjonarne		Sposób realizacji		na odległość (e-learning)		
Rok studiów	4		Język wykładowy		angielski		
Semestr studiów	7		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: 30.0						
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		0.0	30
Cel przedmiotu	Zdobycie przez studenta podstawowej wiedzy o zarządzaniu cyberbezpieczeństwem w organizacjach.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu			Sposób weryfikacji i oceny efektu	
	[K6_W13] ma podstawową wiedzę z zakresu projektowania, modelowania i optymalizacji procesów i systemów technicznych		Student: - opisuje przedsiębiorstwo, - identyfikuje i opisuje zasoby informatyczne przedsiębiorstwa, - rozpoznaje i opisuje problemy cyberbezpieczeństwa przedsiębiorstw, - definiuje środki ochrony.			[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej	
	[K6_U08] analizuje rozwiązania inżynierskie i menedżerskie w procesach podejmowania decyzji z uwzględnieniem aspektów jakościowych i prośrodowiskowych oraz bezpieczeństwa procesów pracy		Student: - analizuje przedsiębiorstwo i jego zasoby informatyczne, - analizuje zagrożenia cyberbezpieczeństwa, - dobiera środki ochrony.			[SU2] Ocena umiejętności analizy informacji [SU1] Ocena realizacji zadania	
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	Znajomość języka angielskiego w stopniu umożliwiającym płynną komunikację						
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)		Próg zaliczeniowy			Składowa oceny końcowej	
	sprawdzian wiedzy		60.0%			45.0%	
	ćwiczenia laboratoryjne		60.0%			50.0%	
	aktywne uczestniczenie w spotkaniach zajęciowych		60.0%			5.0%	

Zalecana lista lektur	Podstawowa lista lektur	1. ISO/IEC 27001:2017 2. NIST SP 800-53 Revision 5 3. Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014. 4. Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html 5. David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011.
	Uzupełniająca lista lektur	1. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 2. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 3. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 4. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 5. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 6. ISO/IEC 15408 (Common Criteria) 7. Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	1. Przeprowadź analizę przedsiębiorstwa. Zidentyfikuj i opisz jego cyberzasoby. 2. Zidentyfikuj niezależne listy zagrożeń cyberbezpieczeństwa i opracuj własną listę cyberzagrożeń. 3. Oszacuj ryzyko cyberbezpieczeństwa. 4. Wyjaśnij systematyczne podejście do zarządzania cyberbezpieczeństwem w przedsiębiorstwie. 5. Wybierz standard cyberbezpieczeństwa, uzasadnij swój wybór. 6. Podaj przykład naruszenia integralności cyberzasobu. 7. Podaj przykład zabezpieczenia służącego zmniejszeniu ryzyko skopiowania danych księgowych przez nieuprawnionych użytkowników. 8. Podaj i wyjaśnij wzór na ryzyko cyberbezpieczeństwa. 9. Wskaż i wyjaśnij najczęstsze strategie postępowania z zagrożeniami związanymi z cyberbezpieczeństwem. 10. Opisz podstawowe cechy kontroli dostępu.	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.