



Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity of Enterprise Infrastructure, PG_00053095							
Kierunek studiów	Inżynieria danych							
Data rozpoczęcia studiów	październik 2024 r.	Rok akademicki realizacji przedmiotu			2026/2027			
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć			Grupa zajęć obowiązkowych z zakresu kierunku studiów 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			angielski			
Semestr studiów	6	Liczba punktów ECTS			3.0			
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin			
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Zarządzania i Ekonomii -> Katedra Informatyki w Zarządzaniu							
Imię i nazwisko wykładowcy (wykładowców)	Od odpowiedzialny za przedmiot	dr hab. inż. Rafał Leszczyna						
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Rafał Leszczyna						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM	
	Liczba godzin zajęć	30.0	0.0	30.0	0.0	0.0	60	
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	60	6.0		9.0		75	
Cel przedmiotu	Nabywanie wiedzy i umiejętności zarządzania infrastrukturą i bezpieczeństwem IT w przedsiębiorstwie							
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu			Sposób weryfikacji i oceny efektu		
	[K6_W04] wykazuje się kreatywnym i przedsiębiorczym działaniem w formułowaniu i realizowaniu innowacyjnych pomysłów		Student wykazuje się kreatywnym i przedsiębiorczym działaniem w analizie oraz szacowaniu ryzyka i kosztów związanych z bezpieczeństwem IT, formułując innowacyjne rozwiązania w zakresie ochrony infrastruktury IT oraz tworzenia dokumentacji bezpieczeństwa, dostosowanych do specyfiki przedsiębiorstwa.			[SW2] Ocena wiedzy zawartej w prezentacji		
	[K6_U02] przygotowuje i przedstawia w sposób przekonujący profesjonalne prezentacje wyników swoich działań, z ich zaawansowaną interpretacją		Student przygotowuje i przedstawia profesjonalne prezentacje wyników analiz związanych z bezpieczeństwem IT, w tym szacowania ryzyka i kosztów			[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU2] Ocena umiejętności analizy informacji		
	[K6_U04] formułuje logiczne rozwiązania złożonych lub nieustrukturyzowanych problemów		Student formułuje logiczne rozwiązania złożonych problemów związanych z bezpieczeństwem IT			[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU2] Ocena umiejętności analizy informacji		

Treści przedmiotu	Treści przedmiotu - wykład		
	<ol style="list-style-type: none"> 1. Wprowadzenie do przedmiotu 2. Infrastruktura IT przedsiębiorstwa 3. Koszt związany z bezpieczeństwem IT 4. Zarządzanie ryzykiem 5. Szacowanie ryzyka 6. Standardy bezpieczeństwa IT 7. Zagrożenia bezpieczeństwa IT 8. Dokumentacja bezpieczeństwa IT w przedsiębiorstwie (m.in. opis infrastruktury IT, opis procedur bezpieczeństwa) 9. Środki ochrony bezpieczeństwa infrastruktury IT 		
Treści przedmiotu - laboratoria	Treści przedmiotu - laboratoria		
	<ol style="list-style-type: none"> 1. Analiza infrastruktury IT przedsiębiorstwa 2. Szacowanie ryzyka 3. Szacowanie kosztu związanego z bezpieczeństwem IT 4. Opracowanie polityki bezpieczeństwa 5. Dobór środków ochrony bezpieczeństwa infrastruktury IT 		
Wymagania wstępne i dodatkowe	Brak wymagań		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Raporty z pracy w laboratorium	60.0%	60.0%
	Egzamin	60.0%	40.0%
Zalecana lista lektur	Podstawowa lista lektur	<ol style="list-style-type: none"> 1. ISO/IEC 27001 2. NIST SP 800-53 3. Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html 4. Ryan Leirvik , Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program, Apress Media, 2023, https://doi.org/10.1007/978-1-4842-9319-5 	
	Uzupełniająca lista lektur	<ol style="list-style-type: none"> 1. Weis, Dan, Boardroom Cybersecurity: A Director's Guide to Mastering Cybersecurity Fundamentals, 2024, Berkeley, CA: Apress L. P 2. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 3. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 4. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 5. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 6. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 7. ISO/IEC 15408 (Common Criteria) 8. Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017 	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<p>Przeanalizuj infrastrukturę IT przedsiębiorstwa a następnie przygotuj jej dokumentację.</p> <p>Przeprowadź analizę ryzyka dla analizowanej infrastruktury IT.</p> <p>Zaproponuj środki bezpieczeństwa dla analizowanej infrastruktury IT.</p> <p>Podaj przykłady infrastruktur krytycznych.</p> <p>Przedstaw i omów podstawowe funkcje zapory sieciowej.</p>		
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.