



Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity of Enterprise Infrastructure, PG_00053095						
Kierunek studiów	Inżynieria danych						
Data rozpoczęcia studiów	październik 2023 r.	Rok akademicki realizacji przedmiotu			2025/2026		
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 odległość (e-learning)		
Rok studiów	3	Język wykładowy			angielski		
Semestr studiów	6	Liczba punktów ECTS			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Wydział 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 inż. Sławomir Ostrowski 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: 60.0						
	Adresy kursu na platformie eNauczanie: Moodle ID: 46152 Cybersecurity of Enterprise Infrastructure 2026 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=46152						
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	Nabycie 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] zna architektury komputerów, procesy systemu operacyjnego, systemy plików, programy do przetwarzania tekstu, zasady zarządzania dyskami i pamięcią ram. zna problemy współdzielenia stanu, prezentacji i transformacji informacji w systemie rozproszonym, technologia hipermediów i związanych z nimi usług, architektury interaktywnej symulacji rozproszonej oraz metody interakcji agentów	Student: - Identyfikuje i opisuje (pod kątem cyberbezpieczeństwa) aktywa infrastruktury informatycznej oraz aktywa informacyjne - Opisuje infrastrukturę informatyczną - Opracowuje schemat infrastruktury informatycznej			[SW1] Ocena wiedzy faktograficznej [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		
[K6_U02] projektuje, analizuje poprawność i tworzy specyfikację funkcjonalną systemów informatycznych, dobierając odpowiednie środki, tworzy modele jakości, przygotowuje i ocenia ich dokumentację projektową	Student: - Analizuje polityki cyberbezpieczeństwa różnych organizacji - Opracowuje dedykowaną politykę cyberbezpieczeństwa - Dobiera i wskazuje cyberzabezpieczenia organizacji w oparciu o wybrane standardy			[SU1] Ocena realizacji zadania [SU2] Ocena umiejętności analizy informacji			

Treści przedmiotu	<p>Treści przedmiotu - wykład WYKŁAD</p> <p>Wprowadzenie do przedmiotu</p> <p>Infrastruktura IT przedsiębiorstwa</p> <p>Koszt związany z bezpieczeństwem IT</p> <p>Zarządzanie ryzykiem</p> <p>Szacowanie ryzyka</p> <p>Standardy bezpieczeństwa IT</p> <p>Zagrożenia bezpieczeństwa IT</p> <p>Dokumentacja bezpieczeństwa IT w przedsiębiorstwie (m.in. opis infrastruktury IT, opis procedur bezpieczeństwa)</p> <p>Środki ochrony bezpieczeństwa infrastruktury IT</p> <p>LABORATORIUM</p> <p>Analiza infrastruktury IT przedsiębiorstwa</p> <p>Szacowanie ryzyka</p> <p>Szacowanie kosztu związanego z bezpieczeństwem IT</p> <p>Stworzenie dokumentacji bezpieczeństwa infrastruktury IT w przedsiębiorstwie</p> <p>Dobór środków ochrony bezpieczeństwa infrastruktury IT</p>		
Wymagania wstępne i dodatkowe	Brak wymagań		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Egzamin	60.0%	45.0%
	Raporty z pracy w laboratorium	60.0%	50.0%
	iso.iec aktywne uczestniczenie w spotkaniach zajęciowych	60.0%	5.0%

Zalecana lista lektur	Podstawowa lista lektur	<p>Ross Anderson, Inżynieria zabezpieczeń, WNT 2005.</p> <p>Adam Gałach, Instrukcja zarządzania bezpieczeństwem systemu Informatycznego, ODDK 2004.</p> <p>Janusz Zawila-Niedźwiecki, Franciszek Wołowski, Bezpieczeństwo systemów informacyjnych:</p> <p>Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Edu-Libri, Kraków - Warszawa, 1, 2012.</p> <p>Krzysztof Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN 2009.</p> <p>Tadeusz Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion 1999.</p>
	Uzupełniająca lista lektur	<p>John Viega, Mity bezpieczeństwa IT: czy na pewno nie masz się czego bać?, Helion 2010.</p> <p>Edward Amoroso, Wykrywanie intruzów, RM 1999.</p> <p>Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 2002.</p> <p>Stuart McClure, Joel Scambray, George Kurtz, Hacking zdemaskowany. Bezpieczeństwo sieci - sekrety i rozwiązania, PWN 2006.</p>
	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.