



Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity Management, PG_00068300						
Kierunek studiów	Zarządzanie inżynierskie (studia w jęz. angielskim)						
Data rozpoczęcia studiów	październik 2025 r.	Rok akademicki realizacji przedmiotu			2027/2028		
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						
	Prowadzący zajęcia z przedmiotu						
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	30.0	0.0	0.0	45
	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	45		5.0		25.0	75
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_K01] jest gotów pełnić role zawodowe w sposób odpowiedzialny, uwzględniając w procesach decyzyjnych kwestie prawne, etyczne i kulturowe.		potrafi podejmować przemyślane decyzje w zakresie ochrony informacji i infrastruktury cyfrowej, z uwzględnieniem konsekwencji prawnych, społecznych i organizacyjnych działań podejmowanych w środowisku cyfrowym		[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce		
	[K6_W03] zna wiarygodne źródła informacji i wykorzystuje zaawansowaną wiedzę do wyjaśniania współczesnych problemów zarządzania.		zna podejścia i źródła informacji, które pozwalają zrozumieć kluczowe wyzwania związane z bezpieczeństwem cyfrowym w organizacjach oraz analizować ich wpływ na funkcjonowanie współczesnych struktur zarządczych.		[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		
	[K6_U06] potrafi zdobywać wiedzę specjalistyczną z zakresu zarządzania inżynierskiego, wykazując umiejętność efektywnego planowania pracy indywidualnej oraz uczenia się przez całe życie.		potrafi samodzielnie poszukiwać i aktualizować wiedzę dotyczącą zagrożeń i praktyk w zakresie bezpieczeństwa cyfrowego, planując efektywnie własny rozwój i reagując na zmieniające się realia technologiczne		[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania [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	Znajomość języka angielskiego w stopniu umożliwiającym płynną komunikację		
Sposoby i kryteria oceniania osiąganych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	ćwiczenia laboratoryjne	60.0%	50.0%
	aktywne uczestniczenie w spotkaniach zajęciowych	60.0%	5.0%
	sprawdzian wiedzy	60.0%	45.0%
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	Adresy na platformie eNauczanie:	
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.