

Karta przedmiotu

Nazwa i kod przedmiotu	Zarządzanie bezpieczeństwem informacji, PG_00063898						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	luty 2026 r.		Rok akademicki realizacji przedmiotu		2026/2027		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć fakultatywnych Grupa zajęć specjalnościowych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		polski		
Semestr studiów	2		Liczba punktów ECTS		3.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Wydział Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Inżynierii Oprogramowania						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr hab. inż. Rafał Leszczyna				
	Prowadzący zajęcia z przedmiotu		dr hab. inż. Rafał Leszczyna				
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	0.0	15.0	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	Celem przedmiotu jest zrozumienie oraz pozyskanie przez studenta wiedzy na temat zarządzania bezpieczeństwem i prywatnością informacji z perspektywy analityka wymagań względem systemów informatycznych						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K7_U02] potrafi wykonywać zadania związane z kierunkiem studiów oraz formułować i rozwiązywać problemy z wykorzystaniem nowej wiedzy z fizyki i innych dziedzin nauki		Student rozumie podstawowe pojęcia związane z analizą ryzyka dotyczącego bezpieczeństwa informacji oraz ochrony przed zagrożeniami bezpieczeństwa i potrafi posłużyć się tymi pojęciami analizując konkretny system IT		[SU2] Ocena umiejętności analizy informacji [SU4] Ocena umiejętności korzystania z metod i narzędzi [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania		
	[K7_W10] zna i rozumie w pogłębionym stopniu podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych oraz metody wspomagania procesów i funkcji, specyficzne dla kierunku studiów		Student rozpoznaje zasoby informacyjne przedsiębiorstwa oraz powiązane zagrożenia. Porządkuje zasoby informacyjne przedsiębiorstwa wg ich stopnia krytyczności. Określa zagrożenia z wykorzystaniem drzew ataków. Definiuje scenariusze możliwych ataków.		[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej		
	[K7_W11] zna i rozumie w pogłębionym stopniu ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości oraz ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z nadaną kwalifikacją, w tym zasady ochrony własności przemysłowej i prawa autorskiego		Student rozumie wpływ zagrożeń bezpieczeństwa informacji oraz prywatności na działalność przedsiębiorstw, a także powiązane z tym uwarunkowania standaryzacyjne i regulacyjne. Charakteryzuje regulacje i zasady dotyczące ochrony prywatności użytkowników. Identyfikuje i przyporządkowuje zabezpieczenia ochrony bezpieczeństwa i prywatności.		[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej		

Treści przedmiotu	1. Zasoby informacyjne I ich znaczenie; 2. Pojęcie i zakres bezpieczeństwa informacji; 3. Bezpieczeństwo a zaufanie; 4. Bezpieczeństwo a użyteczność; 5. Klasyfikacja i etykietowanie zasobów informacyjnych; 6. Ocena zagrożeń i podatności; 7. Ocena ryzyka dotyczącego zasobów informacyjnych; 8. Dobór zabezpieczeń system zarządzania bezpieczeństwem informacji; 9. Wybrane techniki analizy ryzyka drzewa ataków; 10. Standard ISO/IEC 27001:2013 zakres, wymagania, ocena zgodności; 11. Prywatność (pojęcie, zakres, regulacje) oraz wybrane techniki zapewniania prywatności; 12. Relacje między pojęciami bezpieczeństwa (safety), zabezpieczenia (security) i prywatności (privacy); 13. Bezpieczne wytwarzanie oprogramowania 14. Zagrożenia bezpieczeństwa systemów SCADA (Supervisory Control And Data Acquisition).		
Wymagania wstępne i dodatkowe	Wcześniejsze uczestnictwo w przedmiocie <i>Inżynieria wymagań</i>		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Aktywność/obecność	10.0%	10.0%
	Egzamin pisemny	45.0%	45.0%
	Projekt	45.0%	45.0%
Zalecana lista lektur	Podstawowa lista lektur	1. Standard ISO/IEC 27001 2. Standardy IEC/ISA 62443 3. Ross Anderson, Security Engineering, 2-nd edition (dostępny online)	
	Uzupełniająca lista lektur	Standard NIST SP 800-53 Rev. 5 (dostępny online)	
	Adresy eZasobów	Adresy na platformie eNauczanie:	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	1. Przeanalizuj możliwe scenariusze osiągnięcia celów atakującego w systemie informacyjnym. 2. Zaproponuj dodatkowe zabezpieczenia, które chronią przed zidentyfikowanymi atakami. 3. Podaj przykład postaci zasobu informacyjnego. 4. Podaj przykłady 2 typów atrybutów, które można przypisać do węzłów drzewa ataku. 5. Podaj przykład utraty poufności zasobu informacyjnego. 6. Czy zarządzanie ryzykiem powinno być procesem cyklicznym? Uzasadnij swoją odpowiedź. 7. Podaj przykład przeniesienia ryzyka cyberbezpieczeństwa. 8. Jaki jest wiodący międzynarodowy standard SZBI? Podaj peny identyfikator, w tym litery i cyfrę. 9. Jaka jest zalecana dobra praktyka zapewniania prywatności w produktach i modelach biznesowych? 10. Czy ochrona prywatności użytkowników powinna obejmować jakieś zasady? Jeśli tak, to jakie?		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.