



Karta przedmiotu

Nazwa i kod przedmiotu	Zarządzanie bezpieczeństwem sieci, PG_00053895						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	październik 2025 r.	Rok akademicki realizacji przedmiotu		2027/2028			
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		polski			
Semestr studiów	6	Liczba punktów ECTS		3.0			
Profil kształcenia	ogólnoakademicki	Forma zaliczenia		egzamin			
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Krzysztof Gierłowski					
	Prowadzący zajęcia z przedmiotu	dr inż. Krzysztof Gierłowski					
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		1.0		29.0	75
Cel przedmiotu	Celem przedmiotu jest zapoznanie studentów od strony teoretycznej i praktycznej z: • mechanizmami bezpieczeństwa wykorzystywanymi w systemach IT, • rozwiązaniami projektowymi jakie można zastosować w celu podniesienia bezpieczeństwa takich systemów, a także wytworzenie podejścia do bezpieczeństwa rozumianego jako proces ciągły (zarządzania bezpieczeństwem).						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K6_W44] zna i rozumie w zaawansowanym stopniu architektury, zasady projektowania oraz metody wsparcia sprzętowego i programowego dla lokalnych i rozproszonych systemów informatycznych, w tym systemów obliczeniowych, baz danych, sieci komputerowych i aplikacji informacyjnych, zasady współpracy człowieka z komputerem, a także działanie i kryteria oceny metod przetwarzania, składowania i przesyłania danych, w tym algorytmów obliczeniowych, sztucznej inteligencji i eksploracji danych oraz standardy i metody administrowania systemami informatycznymi, monitorowania zachodzących w nich procesów oraz uodporniania ich na niepożądane zjawiska i działania	Student posiada znajomość aktualnych rozwiązań bezpieczeństwa systemów IT, ich cech charakterystycznych, wymagań i funkcjonalności.	[SW1] Ocena wiedzy faktograficznej
	[K6_U07] potrafi wykorzystać metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów	Student posiada znajomość aktualnych rozwiązań bezpieczeństwa systemów IT, potrafi dobierać je zależnie od identyfikowanych zagrożeń.	[SU2] Ocena umiejętności analizy informacji
	[K6_U09] potrafi dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych związanych z kierunkiem studiów i ocenić te rozwiązania, a także wykorzystać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem urządzeń, obiektów i systemów technicznych typowych dla kierunku studiów	Student potrafi skonfigurować poznane mechanizmy bezpieczeństwa stosowane w sieciach komputerowych.	[SU1] Ocena realizacji zadania
Treści przedmiotu	Podstawowe mechanizmy bezpieczeństwa, wymagania dotyczące zarządzania bezpieczeństwem sieci. Filtracja i separacja ruchu sieciowego (VLAN, tunelowanie, firewall). Certyfikaty cyfrowe i PKI. Kryptograficzna ochrona ruchu sieciowego (TLS). Monitorowanie sieci. Rozwiązania kontroli dostępu (RADIUS). Zdalny dostęp (VPN). Wykorzystanie biometrii i kluczy sprzętowych. Rola polityki bezpieczeństwa. Utrzymanie poziomu bezpieczeństwa. Zarządzanie bezpieczeństwem systemów informacyjnych.		
Wymagania wstępne i dodatkowe	Znajomość podstaw funkcjonowania sieci komputerowych (w szczególności sieci IP).		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	laboratorium	50.0%	50.0%
	egzamin pisemny	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2007 r. Liderman K. : Podręcznik administratora bezpieczeństwa sieciowego, Mikom, Warszawa 2003 r. Liderman K. : Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008 r. Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa 2001 r.	

	Uzupełniająca lista lektur	Denning E.: Wojna informatyczna i bezpieczeństwo informacji, WNT, Warszawa 2002 r. Benjamin H. : Cisco CCIE Security, Mikom, Warszawa 2004 r.
	Adresy eZasobów	Adresy na platformie eNauczanie:
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.