



Karta przedmiotu

Nazwa i kod przedmiotu	Kryptografia w cyberbezpieczeństwie, PG_00048039						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	luty 2024 r.	Rok akademicki realizacji przedmiotu			2023/2024		
Poziom kształcenia	II stopnia	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	1	Język wykładowy			polski		
Semestr studiów	1	Liczba punktów ECTS			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Jerzy Konorski					
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Jerzy Konorski					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	0.0	15.0	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	6.0		24.0		75
Cel przedmiotu	Celem przedmiotu jest przekazanie wiedzy i umiejętności związanych z podstawowymi mechanizmami kryptograficznymi. W ramach przedmiotu Studenci poznają podstawy zagrożeń i zabezpieczeń, kryptografii, protokoły kryptograficzne, implementacje i zastosowania kryptografii asymetrycznej - m. in. podpis cyfrowy, znakowanie czasem, PKI. Poruszana jest również tematyka powiązana bezpośrednio z kryptografią, m. in. prywatność i anonimowość, ochrona baz danych, czy elementy kryptografii kwantowej i postkwantowej. Wybrane zagadnienia Studenci mają możliwość poznać praktycznie w ramach zajęć projektowych.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorii, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia		Student zna praktyczne rozwiązania pozwalające osiągnąć określone funkcje bezpieczeństwa.		[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		
	[K7_U42] potrafi rozwiązywać problemy inżynierskie i badawcze w zakresie projektowania, oceny i utrzymania systemów i aplikacji informacyjnych z wykorzystaniem metod eksperymentalnych i technik zarządzania		Student potrafi praktycznie wykorzystać poznane rozwiązania bezpieczeństwa.		[SU4] Ocena umiejętności korzystania z metod i narzędzi		
	[K7_U06] potrafi analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, interpretować uzyskane wyniki i wyciągać wnioski		Student w ramach prac projektowych integruje/ implementuje i prezentuje zastosowanie rozwiązania bezpieczeństwa w określonym scenariuszu użycia.		[SU1] Ocena realizacji zadania		

Treści przedmiotu	Podstawowe pojęcia związane z bezpieczeństwem systemów IT. Metody uwierzytelniania. Wprowadzenie do kryptografii. Kryptografia klucza publicznego i PKI. Usługi kryptograficzne. Protokoły kryptograficzne. Prywatność i anonimowość. Kryptograficzna ochrona baz danych. Elementy protokołów kryptografii kwantowej i postkwantowej.		
Wymagania wstępne i dodatkowe	Znajomość podstaw programowania w języku wysokiego poziomu		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Kolokwium	50.0%	30.0%
	Egzamin	50.0%	30.0%
	Projekt	50.0%	40.0%
Zalecana lista lektur	Podstawowa lista lektur	Materiały i prezentacje do zajęć	
	Uzupełniająca lista lektur	<p>Schneier B.: Kryptografia dla praktyków</p> <p>Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych</p> <p>Stallings W.: Cryptography and Network Security</p> <p>Gollmann D.: Computer security</p>	
	Adresy eZasobów	Adresy na platformie eNauczanie: Kryptografia w cyberbezpieczeństwie 2024 - Moodle ID: 29474 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=29474	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		