

"ZATWIERDZAM"

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Podstawy kryptologii współczesnej			Foundations of modern cryptology				
Kod przedmiotu	WCYKBWSM_PKW.....							
Język wykładowy	polski							
Profil studiów	ogólnoakademicki							
Forma studiów	studia stacjonarne							
Poziom studiów	wojskowe studia jednolite magisterskie							
Rodzaj przedmiotu								
Obowiązuje od naboru	2021/2022							
Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS	semestr	(x egzamin, + zaliczenie, # projekt)					punkty ECTS	
		razem	wykłady	ćwiczenia	laboratoria	projekt		seminarium
	VIII	44+	16	12+	16+			3.0
	razem		16	12	16			3.0
Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających							
Semestr/kierunek studiów	semestr 8 / Kryptologia i cyberbezpieczeństwo / Bezpieczeństwo informacyjne							
Autor	mgr inż. Krzysztof Kanciak							
Jednostka odpowiedzialna za przedmiot	IMK							
Skrócony opis przedmiotu	• wykład z możliwym wykorzystaniem technik audiowizualnych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania • ćwiczenia rachunkowe ułatwiające opanowanie, zrozumienie i usystematyzowanie wiedzy wyniesionej z wykładów i własnych studiów studentów • zajęcia laboratoryjne z indywidualnymi zajęciami (preferowana forma pozwalająca na tryb zdalny)							
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VIII temat/tematyka zajęć			liczba godzin			
			wkl.	ćw.	lab.	prj.	sem.	
	1	Teoria informacji oraz teoria złożoności w kontekście współczesnej kryptografii. Wprowadzenie do wykładu.			4	2	2	
	2	Bezpieczeństwo idealne, statystyczne, obliczeniowe. Definicje, modele bezpieczeństwa.			4	2	2	
	3	Analiza teoretycznych i praktycznych przypadków prymitywów kryptograficznych			2	2	4	
	4	Współczesne zastosowania kryptografii. Protokoły kryptograficzne.			2	4	4	
	5	Zaawansowane zagadnienia współczesnej kryptografii.			4	2	4	
	Razem			16	12	16		
Literatura	podstawowa:							
	• Introduction to Modern Cryptography; Chapman & Hall/CRC Cryptography and Network Security Series 2nd Edition; Jonathan Katz, Yehuda Lindell; ISBN-13: 978-1466570269 • R. Stinson "Kryptografia W teorii i praktyce" PWN 2021. • Elementy teoretycznych podstaw informatyki, Marian Chudy, 83-60434-10-7, 978-83-7837-538-8 uzupełniająca: • Menezes, P. van Oorschoot, S. Vanstone "Kryptografia stosowana" WNT, Warszawa 2006. • Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania. Aumasson Jean-Philippe, 2018 PWN • Szmidt J., Misztal M.; Wstęp do kryptologii; WSISiZ, 2001 • Understanding Cryptography: A Textbook for Students and Practitioners; by Christof Paar, Jan Pelzl, Bart Preneel, 2010; ISBN-10: 3642041000							
Efekty uczenia się	Symbol	Efekty kształcenia				odniesienie do efektów kształcenia dla kierunku		
	W1	zna i rozumie/posiada uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą podstaw współczesnej kryptografii				K_W04, K_W08, K_W09		
	K1	jest gotów do krytycznej oceny posiadanej wiedzy i jej znaczenia w rozwiązywaniu problemów poznawczych i praktycznych.				K_U12, K_W03, K_W12		
	U1	potrafi posługiwać się w podstawowym zakresie językiem oraz metodami wykorzystania współczesnych systemów, metod, technik ochrony bezpieczeństwa systemów informatycznych.				K_U03, K_U10, K_U15		

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie egzaminu. Egzamin jest przeprowadzamy w formie pisemnej lub ustnej. • Laboratorium zaliczane jest na podstawie samodzielnej pracy zaliczeniowej lub prac cząstkowych. • Warunkiem koniecznym uzyskania zaliczenia laboratorium jest obecność na co najmniej 81% zajęć. • Warunkiem dopuszczenia do egzaminu jest zaliczenie laboratorium.		
Bilans ECTS (nakład pracy studenta)	SEMESTR 8		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	16	0.5
	Udział w laboratoriach	16	0.5
	Udział w ćwiczeniach	12	0.5
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	20	0.5
	Samodzielne przygotowanie do laboratoriów	10	0.5
	Samodzielne przygotowanie do ćwiczeń	20	0.5
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia		
	Udział w egzaminie / kolokwium		
	Sumaryczne obciążenie pracą studenta	94	3
	Zajęcia z udziałem nauczycieli	44	1.5
	Zajęcia powiązane z działalnością naukową	94	3
	Zajęcia o charakterze praktycznym	58	2

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

mgr inż. Krzysztof Kanciak

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis