

"ZATWIERDZAM"

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Steganografia		Steganography							
Kod przedmiotu	WCYKSWSM									
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		
	IX	30+	16	14+					3.0	
	razem		16	14				3.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / wszystkie specjalności									
Autor	mgr inż. Kamil Kaczyński									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki / Instytut Matematyki i Kryptologii / Pracownia Matematyki Stosowanej									
Skrócony opis przedmiotu	● wykład z możliwym wykorzystaniem technik audiowizualnych ● zajęcia w laboratorium komputerowym z wykorzystaniem dedykowanego oprogramowania, ułatwiające opanowanie, zrozumienie i usystematyzowanie wiedzy wyniesionej z wykładów i własnych studiów studentów ● podanie zadań do samodzielnego rozwiązania i tematów do studiowania									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IX temat/tematyka zajęć				liczba godzin				
						wkl.	ćw.	lab.	prj.	sem.
	1	Wprowadzenie. Rys historyczny steganografii. Podstawowe pojęcia. Steganografia z kluczem publicznym i kluczem prywatnym. Cyfrowe znaki wodne.				2				
	2	Steganografia w obrazach. Podstawowe algorytmy steganograficzne dla grafiki rastrowej - LSB, F5, JSteg. Algorytmy dla kompresji stratnej i bezstratnej.				4	6			
	3	Steganografia audio/wideo. Algorytmy dla zastosowań w plikach multimedialnych. Kompresja stratna i bezstratna.				2	2			
	4	Steganografia sieciowa. Algorytmy ukrywania informacji w protokole TCP/IP oraz danych strumieniowanych.				2	2			
	5	Stegoanaliza. Stegoanaliza wizualna i statystyczna. Test chi-kwadrat, algorytm RS. Metody stegoanalizy uniwersalnej				4	4			
	6	Kodowanie macierzowe. Wet Paper Codes.				2				
	Razem				16	14				
Literatura	podstawowa: ● S. Katzenbeisser, Information Hiding Techniques for Steganography and Digital Watermarking, 1999 ● I. Cox, J. Fridrich, Digital Watermarking and Steganography, 2007 ● W. Mosorow, Steganografia cyfrowa. Sztuka ukrywania informacji, 2014 uzupełniająca: ● G. Kipper, Investigator's Guide to Steganography, 2003 ● E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, 2003 ● P. Wayner, Disappearing cryptography. Information hiding: steganography & watermarking, 2009									
Efekty uczenia się	Symbol	Efekty kształcenia				odniesienie do efektów kształcenia dla kierunku				
	W1	Zna podstawowe algorytmy steganograficzne. Poznał i rozumie różnice pomiędzy kryptografią, steganografią a cyfrowym znakowaniem wodnym. Zna podstawowe typy strażników w systemach steganograficznych. Poznał najczęściej stosowane metody stegoanalityczne.				K_W02, K_W22, K_W23				
	U1	Umie posługiwać się podstawowym językiem steganografii i stegoanalizy. Umie wykorzystywać podstawowe kody korekcji błędów, a także stosować rachunek macierzowy do ukrywania danych. Umie tworzyć elementarne algorytmy steganograficzne.				K_U19, K_U20				

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
	U2	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie.	K_U11	
	K1	Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze steganografią i bezpieczeństwem danych.	K_K01	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie pracy kontrolnej sprawdzającej wiedzę (W1) i umiejętności (U1, U2). Egzamin może mieć formę pisemną i/lub ustną. • Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń laboratoryjnych. • Ćwiczenia laboratoryjne zaliczane są na podstawie wyników prac kontrolnych przeprowadzanych pod bezpośrednią kontrolą podczas zajęć (U1, U2, W1) lub w formie zadań do samodzielnego rozwiązania (K1, U2, U1). • Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie zastosować podstawowe algorytmy steganograficzne; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie budować i analizować algorytmy steganograficzne, potrafi wyszukiwać nośniki steganograficzne, potrafi zastosować proste algorytmy stegoanalityczne; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie budować i stosować zaawansowane algorytmy steganograficzne, potrafi analizować nośniki w poszukiwaniu ukrytych informacji; dość dobrze (3,5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 9			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	16	1	
	Udział w laboratoriach	0	0	
	Udział w ćwiczeniach	14	1	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	30	1	
	Samodzielne przygotowanie do laboratoriów			
	Samodzielne przygotowanie do ćwiczeń	20		
	Samodzielna realizacja projektu			
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia			
	Udział w egzaminie / kolokwium	15		
	Sumaryczne obciążenie pracą studenta	95	3	
	Zajęcia z udziałem nauczycieli	45	2	
	Zajęcia powiązane z działalnością naukową	80	3	
Zajęcia o charakterze praktycznym	34	1		

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

mgr inż. Kamil Kaczyński

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis