

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Certyfikacja urządzeń kryptograficznych				Certification of cryptographic equipment					
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			
	X	30+	10		20+			2.0		
	razem		10		20			2.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 10 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	dr inż. Piotr Bora, mgr inż. Łukasz Dziół									
Jednostka odpowiedzialna za przedmiot	WCY/IMiK/ZK									
Skrócony opis przedmiotu	● Wykłady i ćwiczenia laboratoryjne									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr X temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Ogólne zasady konstrukcji urządzeń kryptograficznych LAB-01: IP, Zadanie, Analiza wymagań biznesowych; LAB-02: Wymagania funkcjonalne i нефункционалне;				2		4		
	2	Ogólne zasady konstrukcji systemów kryptograficznych LAB-03: Projekt Systemu Kryptograficznego;				2		2		
	3	Historia i praktyki realizacji oceny bezpieczeństwa od "Orange Book" przez ITSEC po Wspólne Kryteria - Norma PN-ISO/IEC 15408-1, FIPS PUB 140 LAB-04: FIPS-140-2: Cryptographic Module Specification, Ports and Interfaces; LAB-05: FIPS-140-2: Roles, Services, and Authentication; LAB-06: FIPS-140-2: Finite State Model; LAB-07: FIPS-140-2: Physical Security, Operational Environment; LAB-08: FIPS-140-2: Cryptographic Key Management; LAB-09: FIPS-140-2: Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC), Self-Tests; LAB-10: FIPS-140-2: Mitigation of Other Attacks;				6		14		
	Razem				10		20			
Literatura	podstawowa:									
	● Krzysztof Liderman Bezpieczeństwo teleinformatyczne 2001									
	uzupełniająca:									
	● Rozporządzenie MSWiA z dnia 3.06.1998, Dz. U. 30.06.1999 ● ISO/IEC 15408 "Evaluation criteria for information technology security" ● Normy PN ISO/IEC z zakresu Technika informatyczna - Techniki zabezpieczeń									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku			
	U1	Umie formułować, analizować problemy, znajdować ich rozwiązania oraz przeprowadzać eksperymenty, interpretować ich wyniki i wyciągać wnioski w zakresie rozwiązań bezpieczeństwa systemów teleinformatycznych.					K_U11, K_U19			
	U2	Umie analizować i oceniać bezpieczeństwo systemów kryptograficznych					K_U11, K_U19			
	W1	Zna i rozumie pojęcia oraz zasady i metody konstrukcji i analizy poprawności protokołów i algorytmów kryptograficznych i kryptoanalitycznych					K_W23			

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	Ocena końcowa z modułu kształcenia jest wystawiana na podstawie oceny z zajęć praktycznych; Podczas zajęć zdalnych jest obowiązek włączenia (na żądanie) mikrofonu i kamery, oraz wyświetlenia opracowanych podczas zajęć materiałów; Podczas zajęć stacjonarnych jest obowiązek udostępnienia (na żądanie) opracowanych podczas zajęć materiałów; Do zajęć uruchamiany jest zespół na platformie Microsoft Teams w celu: udostępniania materiałów do zajęć, przekazywania Rozwiązań Zadań Indywidualnych, oraz zapewnienia sprawnego kontaktu i konsultacji; Zajęcia zaliczane są na podstawie Rozwiązań Zadań Indywidualnych (RZI), weryfikacji samodzielności ich wykonania oraz Aktywności Podczas Zajęć (APZ); Zadania Indywidualne dotyczą każdego z zajęć praktycznych lub etapów zadania projektowego i polegają na przedstawieniu swojej pracy oraz rozwiązań praktycznych problemów dotyczących tematyki zajęć; Samodzielność wykonania RZI jest weryfikowana poprzez: analizę (w tym porównawczą) napisanych prac, odpowiedzi pisemne lub ustne podczas zajęć w trakcie semestru lub w terminach sesji, w formie stacjonarnej lub zdalnej, niezależnie od formy prowadzenia zajęć; RZI są oceniane w skali: ZAL - (1 punkt) - w przypadku, gdy rozwiązanie zadania jest prawidłowe, lub wykonane starannie i zawiera nieistotne błędy lub niewielkie braki, NZAL - (0 punktów) - w przeciwnym przypadku. Ostateczne terminy przesłania RZI lub ich popraw, które umożliwiają uzyskanie oceny w poszczególnych terminach zaliczenia, są podane w zespole Microsoft Teams uruchomionym do zajęć; Aktywność Podczas Zajęć dotyczy każdego z zajęć praktycznych lub etapów zadania projektowego i polega na aktywnym braniu udziału w zajęciach, w szczególności poprzez dyskusję nad problemami i rozwiązywaniu zadań podczas zajęć; Aktywność Podczas Zajęć jest oceniana zgodnie z następującymi wytycznymi: 1 punkt - udzielanie istotnej liczby poprawnych odpowiedzi podczas zajęć lub etapu zadania projektowego, 0 punktów - w przeciwnym przypadku; Aktywności Podczas Zajęć się nie poprawia; Ocena końcowa z zajęć praktycznych we wszystkich terminach jest wystawiana na podstawie ilorazu sumy uzyskanych punktów z Rozwiązań Zadań Indywidualnych i Aktywności Podczas Zajęć oraz liczby zajęć lub etapów zadania projektowego, z dokładnością do dwóch miejsc po przecinku w następujący sposób: 0.00 i w przypadku nieoddania żadnego z RZI - NB; od 0.01 do 0.99 - 2 (ndst); od 1.00 do 1.11 - 3. 0 (dst); od 1.12 do 1.23 - 3.5 (dst+); od 1.24 do 1.35 - 4.0 (db); od 1.36 do 1.47 - 4.5 (db+); od 1.48 do 2. 00 - 5.0 (bdb).																																																														
Bilans ECTS (nakład pracy studenta)	<table><tr><th colspan="3">SEMESTR 10</th></tr><tr><th rowspan="2">Aktywność</th><th colspan="2">Obciążenie studenta</th></tr><tr><th>Liczba godzin</th><th>Liczba ECTS</th></tr><tr><td>Udział w wykładach</td><td>10</td><td>0.2</td></tr><tr><td>Udział w laboratoriach</td><td>20</td><td>0.4</td></tr><tr><td>Udział w ćwiczeniach</td><td></td><td></td></tr><tr><td>Udział w projektach</td><td></td><td></td></tr><tr><td>Udział w seminariach</td><td></td><td></td></tr><tr><td>Samodzielne studiowanie tematyki wykładów</td><td>10</td><td>0.4</td></tr><tr><td>Samodzielne przygotowanie do laboratoriów</td><td>30</td><td>1.0</td></tr><tr><td>Samodzielne przygotowanie do ćwiczeń</td><td></td><td></td></tr><tr><td>Samodzielna realizacja projektu</td><td></td><td></td></tr><tr><td>Samodzielne przygotowanie do seminariów</td><td></td><td></td></tr><tr><td>Udział w konsultacjach</td><td></td><td></td></tr><tr><td>Przygotowanie do egzaminu</td><td></td><td></td></tr><tr><td>Przygotowanie do zaliczenia</td><td></td><td></td></tr><tr><td>Udział w egzaminie / kolokwium</td><td></td><td></td></tr><tr><td>Sumaryczne obciążenie pracą studenta</td><td>70</td><td>2</td></tr><tr><td>Zajęcia z udziałem nauczycieli</td><td>30</td><td>0.6</td></tr><tr><td>Zajęcia powiązane z działalnością naukową</td><td>70</td><td>2</td></tr><tr><td>Zajęcia o charakterze praktycznym</td><td>50</td><td>1.4</td></tr></table>	SEMESTR 10			Aktywność	Obciążenie studenta		Liczba godzin	Liczba ECTS	Udział w wykładach	10	0.2	Udział w laboratoriach	20	0.4	Udział w ćwiczeniach			Udział w projektach			Udział w seminariach			Samodzielne studiowanie tematyki wykładów	10	0.4	Samodzielne przygotowanie do laboratoriów	30	1.0	Samodzielne przygotowanie do ćwiczeń			Samodzielna realizacja projektu			Samodzielne przygotowanie do seminariów			Udział w konsultacjach			Przygotowanie do egzaminu			Przygotowanie do zaliczenia			Udział w egzaminie / kolokwium			Sumaryczne obciążenie pracą studenta	70	2	Zajęcia z udziałem nauczycieli	30	0.6	Zajęcia powiązane z działalnością naukową	70	2	Zajęcia o charakterze praktycznym	50	1.4
SEMESTR 10																																																															
Aktywność	Obciążenie studenta																																																														
	Liczba godzin	Liczba ECTS																																																													
Udział w wykładach	10	0.2																																																													
Udział w laboratoriach	20	0.4																																																													
Udział w ćwiczeniach																																																															
Udział w projektach																																																															
Udział w seminariach																																																															
Samodzielne studiowanie tematyki wykładów	10	0.4																																																													
Samodzielne przygotowanie do laboratoriów	30	1.0																																																													
Samodzielne przygotowanie do ćwiczeń																																																															
Samodzielna realizacja projektu																																																															
Samodzielne przygotowanie do seminariów																																																															
Udział w konsultacjach																																																															
Przygotowanie do egzaminu																																																															
Przygotowanie do zaliczenia																																																															
Udział w egzaminie / kolokwium																																																															
Sumaryczne obciążenie pracą studenta	70	2																																																													
Zajęcia z udziałem nauczycieli	30	0.6																																																													
Zajęcia powiązane z działalnością naukową	70	2																																																													
Zajęcia o charakterze praktycznym	50	1.4																																																													

autorzy

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Piotr Bora
tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek
tytuł, stopień naukowy, imię, NAZWISKO, podpis

mgr inż. Łukasz Dzieł
tytuł, stopień naukowy, imię, NAZWISKO, podpis