

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Oprogramowanie niepożądane i inspekcja kodu							Malware and binary code inspection		
Kod przedmiotu	WCYKCCSI_TIM.....TIM									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	studia pierwszego stopnia									
Rodzaj przedmiotu	obowiązkowy									
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			
	VI	44+	14		14+	16+		4.0		
	razem		14		14	16		4.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 6 / Kryptologia i cyberbezpieczeństwo / Cyberobrona									
Autor	dr inż. Adam Patkowski									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/Instytut Teleinformatyki i Cyberbezpieczeństwa/ZSK									
Skrócony opis przedmiotu	● Wykład przy komputerach ● Ćwiczenia laboratoryjne									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VI temat/tematyka zajęć				liczba godzin				
						wkl.	ćw.	lab.	prj.	sem.
	1	Wprowadzenie. Klasyfikacje i zasady bezpieczeństwa.				2				
	2	Narzędzia budowy i inspekcji kodów binarnych.				2		4	8	
	3	Architektura IA-32 i x64, komunikacja z SO - powtórzenie wybranych treści.				4				
	4	Budowa malware. Typowe funkcje, tricki, ukrywanie przed AV, polimorfizm. msfvenom				2		2	4	
	5	Sposoby inwazji. Social engineering. Poczta. Exploity.				2		4	2	
	6	Narzędzia ataków złożonych i kampanii phishingowych. RATs. Meterpreter. Ataki "u wodopoju". Ransomware.				2		4	2	
	Razem				14		14	16		
Literatura	podstawowa: ● Dokumentacje techniczne procesorów 32-bitowych Intel i AMD, np. z Intel® 64 and IA-32 Architectures Software Developer Manuals ● Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sébastien Josse: Inżynieria odwrotna w praktyce. Narzędzia i techniki. Helion 2015. ● Rapis7: Metasploit (aktualny stan projektu) ● Hyde Randall: The Art of Assembly Language Programming. ● MITRE ATT&CK uzupełniająca: ● Dennis Yurichev: Reverse Engineering for Beginners ● Dr Xiang Fu: Malware Analysis Tutorials: a Reverse Engineering Approach ● Sekurak: Statyczna analiza bezpieczeństwa kodu aplikacji ● Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sébastien Josse: Inżynieria odwrotna w praktyce. Narzędzia i techniki. Helion 2014.									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku			
	W13	Znajomość klasyfikacji niepożądanego oprogramowania i sposobów jego budowy					K_W14			
	U45	Umiejętność posługiwania się narzędziami statycznej i dynamicznej inspekcji kodu					K_W14, K_U12			
	U6	Umiejętność identyfikacji oprogramowania niepożądanego i jego bezpiecznego badania					K_W14, K_U12			

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie oceny z kolokwium oraz oceny z ćwiczeń (obie muszą być pozytywne) • Ćwiczenia zaliczane są na podstawie ocen bieżących z laboratoriów przy obowiązku min. 80% obecności. • Efekt W13 sprawdzany jest za pomocą kolokwium, efekty U6 i U45 na podstawie realizacji ćwiczeń laboratoryjnych oraz projektu.		
Bilans ECTS (nakład pracy studenta)	SEMESTR 6		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	14	1
	Udział w laboratoriach	14	1
	Udział w ćwiczeniach	0	0
	Udział w projektach	16	1
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	16	
	Samodzielne przygotowanie do laboratoriów		
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu	48	1
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia		
	Udział w egzaminie / kolokwium		
	Sumaryczne obciążenie pracą studenta	108	4
	Zajęcia z udziałem nauczycieli	44	3
	Zajęcia powiązane z działalnością naukową	108	4
	Zajęcia o charakterze praktycznym	78	3

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Adam Patkowski

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr inż. Malinowski Tomasz

tytuł, stopień naukowy, imię, NAZWISKO, podpis