"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Techniki dochodzeniowe i śledcze	Investigative techniques
Kod przedmiotu	WCYKCWSM_.....	
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	30+	10		20+			3.0
razem		10		20			3.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 8 / Kryptologia i cyberbezpieczeństwo / Cyberobrona
Autor	dr inż. Adam Patkowski
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/Instytut Teleinformatyki i Cyberbezpieczeństwa/ZSK
Skrócony opis przedmiotu	• Wykład • Ćwiczenia laboratoryjne

Pełny opis przedmiotu (treści programowe)

lp.	Semestr VIII temat/tematyka zajęć	liczba godzin				
		wkł.	ćw.	lab.	prj.	sem.
1	Cele, podstawowe zasady i obszar działań informatyki śledczej. Dokumentacja.	1				
2	Lokalizacja zasobów informacyjnych użytecznych do celów dowodowych.	1				
3	Podstawy i narzędzia pozyskiwania danych. Zabezpieczanie danych - obrazy nośników i zrzutów pamięci.	2		4		
4	Narzędzia do działań śledczych.	2		4		
5	Metody analizy danych. Wnioskowanie. Case studies.	2		8		
6	Wykrywanie malware i modyfikacji kodu. Analiza kodu.	2		4		
	Razem	10		20		

Literatura

podstawowa:
- Luttgens J., Pepe M., Mandia K.: Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej. Helion 2016.
- Carvey H.: Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7. Wyd. III. Helion 3013.
- ENISA.: Digital forensics Handbook, Document for teachers. September 2013.
- CAINE - Computer Forensics Live Distro http://www.caine-live.net/ - aktualny stan projektu

uzupełniająca:
- Kalinowski Artur M.: Metody inwigilacji i elementy informatyki śledczej. CSH 2011.
- Ziaja A.: Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux. PWN 2017.
- Kosiński J.: Przestępczość teleinformatyczna. WSPol rok 2015 i następne. Wybrane rozdziały.
- Katana WAT blade - aktualny stan projektu

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W1	Znajomość podstawowych metod, techniki i narzędzi do zabezpieczania elektronicznego materiału dowodowego	K_U11, K_K05
W2	Znajomość typowych lokalizacji (w popularnych systemach) informacji potencjalnie użytecznych procesowo	K_W14
W3	Umiejętność podstawowej analizy powłamaniowej - identyfikacji zdarzeń na podstawie stanu zasobów informacyjnych komputerów	K_W08, K_W14, K_U11
W4	Umiejętność wykrywania i analizy malware o różnym stopniu komplikacji	K_U11, K_W08
W5	Umiejętność rozpoznania przesłanek działań przestępczych i podjęcia decyzji o krokach prawnych	K_W14, K_W08, K_U11

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Efekty W1 i W2 sprawdza się w trakcie kolokwium końcowego. • Efekty W3-W5 sprawdzane są na zajęciach laboratoryjnych.

Bilans ECTS (nakład pracy studenta)

SEMESTR 8		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	10	1
Udział w laboratoriach	20	2
Udział w ćwiczeniach	0	0
Udział w projektach	0	0
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	20	
Samodzielne przygotowanie do laboratoriów	40	
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	90	3
Zajęcia z udziałem nauczycieli	30	3
Zajęcia powiązane z działalnością naukową	90	3
Zajęcia o charakterze praktycznym	60	2

autor

dr inż. Adam Patkowski
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr inż. Malinowski Tomasz
tytuł, stopień naukowy, imię, NAZWISKO, podpis