"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Walka w cyberprzestrzeni	Cyberspace fighting
Kod przedmiotu	WCYKCWSM_.....	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	wojskowe studia jednolite magisterskie	
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	
X	30x	10		20+			3.0
razem		10		20			3.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 10 / 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 X temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Walka informacyjna. Podstawowe pojęcia cyberbezpieczeństwa. Sieci rozległe i organizacja Internetu. Cele w cyberprzestrzeni (infrastruktura krytyczna, zasoby korporacyjne, media społecznościowe, urządzenia prywatne). Dezinformacja jako narzędzie polityki, strategii, biznesu i spekulacji.	2				
2	Ataki na stację roboczą i jej użytkownika. Malware. Obrona.	2		6		
3	Wydobywanie informacji. Media społecznościowe. OSINT. Oddziaływania masowe. Botnety i ataki Sybil. Kontrataki.	2		4		
4	Ataki na systemy teleinformatyczne organizacji.	2		8		
5	Wielkoskalowe ataki DDoS. Dezinformacja. Obrona cyberprzestrzeni kraju.	2		2		
	Razem	10		20		

Literatura

podstawowa:
- Aktualne materiały z Internetu
- Dela Piotr: Teoria walki w cyberprzestrzeni. Akademia Sztuki Wojennej. Warszawa 2020.
- Publikacje ENISA https://www.enisa.europa.eu/
- Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure. Executive Office of the President of The US 2009.
- Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. (z https://www.gov.pl)

uzupełniająca:
- Doktryna bezpieczeństwa Rzeczypospolitej Polskiej. https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf
- Kali Linux (aktualny stan projektu i powiązanych, wg http://kali.org)
- Rapd7: Metasploit (aktualny stan projektu wg https://www.metasploit.com/)
- OSINT Framework http://osintframework.com/
- Baza https://www.exploit-db.com
- Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94.
- MITRE: Making Security Measurable; https://makingsecuritymeasurable.mitre.org/

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W01	Znajomość organizacji Internetu i celów wrogich oddziaływań w cyberprzestrzeni.	K_K03, K_K05, K_W08, K_U11
W02	Znajomość sposobów zapewniania sobie cyberbezpieczeństwa.	K_U11, K_W14
W03	Znajomość taktyki walki informacyjnej.	K_U11, K_W14
W45	Znajomość ogólnych sposobów prowadzenia cyberataków i metod obrony przed nimi.	K_K05, K_U11

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
	U01	Umiejętność rozpoznania symptomów i identyfikacji wrogich działań.	K_U11, K_W08
	U02	Umiejętność obrony osobistej stacji roboczej przed cyberatakami.	K_U11
	U23	Umiejętność zapewnienia prywatności i poufności własnych zasobów informacyjnych oraz komunikacji.	K_U11, K_W08, K_W14
	U45	Umiejętność wskazania możliwości ataku lub oddziaływania w cyberprzestrzeni dla osiągnięcia wybranych celów.	K_K05, K_K03, K_W14, K_W08

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Ocena z przedmiotu wystawiana jest na podstawie wyniku egzaminu problemowego: po krótkim przygotowaniu odpowiadający przedstawia rozwiązanie postawionego problemu z jego ewentualną obroną w dyskusji z egzaminatorem.
- Warunkiem dopuszczenia do egzaminu jest Pozytywna ocena z ćwiczeń laboratoryjnych.
- Ocena z ćwiczeń laboratoryjnych wystawiana jest na podstawie obecności i ocen bieżących z zadań laboratoryjnych.
- Warunkiem zaliczenia ćwiczeń laboratoryjnych jest udział w co najmniej 14 (z 20) godzinach tych zajęć.
- Efekty U01, U02, U23, U45 są osiągane i weryfikowane w trakcie ćwiczeń laboratoryjnych.
- Efekty W01, W02, W03, W45, U01, U45 są weryfikowane na egzaminie.

Bilans ECTS (nakład pracy studenta)

SEMESTR 10

Aktywność	Obciążenie studenta	
	Liczba godzin	Liczba ECTS
Udział w wykładach	10	1
Udział w laboratoriach	20	1
Udział w ćwiczeniach		
Udział w projektach		
Udział w seminariach		
Samodzielne studiowanie tematyki wykładów	20	
Samodzielne przygotowanie do laboratoriów		
Samodzielne przygotowanie do ćwiczeń	48	1
Samodzielna realizacja projektu		
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu		
Przygotowanie do zaliczenia		
Udział w egzaminie / kolokwium		
Sumaryczne obciążenie pracą studenta	98	3
Zajęcia z udziałem nauczycieli	30	2
Zajęcia powiązane z działalnością naukową	98	3
Zajęcia o charakterze praktycznym	68	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