

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Podstawy zabezpieczeń sieci						Basis of networks security	
Kod przedmiotu	WCYIRWSM_PZS							
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	
	VI	44x	18		26+			3.0
	razem		18		26			3.0
Przedmioty wprowadzające	Brak przedmiotów kształcenia wprowadzających							
Semestr/kierunek studiów	semestr 6 / Informatyka / Systemy teleinformatyczne - bezpieczeństwo systemów teleinformatycznych							
Autor	mgr inż. Łukasz Laszko							
Jednostka odpowiedzialna za przedmiot	WCY / ITC / ZBT							
Skrócony opis przedmiotu	- Wykłady przeprowadzane z wykorzystaniem środków audiowizualnych jako elementów wspomagających - Samodzielne studiowanie zaleconej literatury - Ćwiczenia laboratoryjne polegające na samodzielnym realizowaniu czynności związanych z badaniem wybranych mechanizmów bezpieczeństwa sieci - Opracowywanie sprawozdań-raportów ze zrealizowanych ćwiczeń laboratoryjnych - Bieżące sprawdzanie zakresu opanowania fragmentów materiału niezbędnego do poprawnego realizowania ćwiczeń laboratoryjnych - Końcowe sprawdzanie zakresu opanowania materiału przedmiotu realizowane w formie egzaminu							
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VI temat/tematyka zajęć	liczba godzin					
			wkt.	ćw.	lab.	prj.	sem.	
	1	Wstęp, podstawowe pojęcia dotyczące bezpieczeństwa informacji, pasywne techniki testów penetracyjnych.	3					
	2	Aktywne techniki eksploracji sieci (skanowanie, identyfikacja systemów operacyjnych, enumeracja)	4		12			
	3	Ataki sieciowe	2		2			
	4	Techniki kryptograficzne i PKI	3		4			
	5	Bezpieczne protokoły sieciowe	3		4			
	6	Zapory sieciowe i wykrywanie intruzów	3		4			
		Razem	18		26			
Literatura	podstawowa: - Pillay R., Learn Penetration Testing Packt Publishing Ltd, 2019. - Allen L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing Ltd, 2016. - Adams C., Lloyd S., PKI: Podstawy i zasady działania, PWN 2007 - Serafin M., Sieci VPN. Zdalna praca i bezpieczeństwo danych, Helion 2013. - Suski Z., Techniki skanowania. Rozdz. 10 w monografii Bezpieczeństwo teleinformatyczne - problemy formalne i techniczne, WAT 2006. - Suski Z., Rekonesans pasywny w testach penetracyjnych, Przegląd Teleinformatyczny (3), 2017 - Suski Z., Wybrane przypadki enumeracji systemu Windows Server 2012, Przegląd Teleinformatyczny 1-2/2014, Instytut Teleinformatyki i Automatyki WAT, Warszawa 2014. - Suski Z., Wybrane aspekty bezpieczeństwa DNS. Biuletyn WAT (4) 2011. uzupełniająca: - Baloch R., 2010. Ethical Hacking and Penetration Testing Guide, CRC Press 2015. - Scambray J., McClure S., Kurtz G., Hacking Exposed, 7th Edition, McGraw Hill 2012. - Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. NIST 2007 - Scarfone K., Hoffman P., Guidelines on Firewalls and Firewall Policy. NIST 2009.							

Efekty uczenia się	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
	W1	Zna i rozumie pojęcia, zasady i metody z zakresu funkcjonowania sieci komputerowych i użytkowania podstawowych usług sieciowych oraz szczegółową wiedzę z zakresu administrowania sieciami systemami operacyjnymi. Zna podstawowe zagrożenia bezpieczeństwa informacji w sieciach komputerowych.	K_W14	
	W2	Zna podstawowe mechanizmy zabezpieczania informacji w sieciach komputerowych, w tym podstawowe pojęcia i metody z zakresu technik kryptograficznych i systemów zabezpieczeń	K_W14	
	U1	potrafi planować i przeprowadzać eksperymenty z zakresu ochrony zasobów dostępnych przez sieci teleinformatyczne, interpretować uzyskane wyniki i wyciągać wnioski, ocenić przydatność rutynowych metod i narzędzi zabezpieczania sieci oraz wybrać i zastosować właściwą metodę, zaprojektować i wdrożyć podstawowe elementy systemu zarządzania bezpieczeństwem informacji	K_U12	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Zaliczenie ćwiczeń laboratoryjnych odbywa się na podstawie sumy punktów uzyskanych za realizację zadań bieżących (ocenianych na podstawie sprawozdań-raportów) i sprawdziany bieżące ("wejściówki"). Nie uzyskują zaliczenia ćwiczeń laboratoryjnych studenci, którzy nie zaliczyli ponad 20% sprawozdań laboratoryjnych. Status sprawozdania zaliczonego uzyskuje opracowanie, za które uzyskano co najmniej 50% punktów. Nie będą przyjmowane sprawozdania od osób, które nie uczestniczyły w zajęciach laboratoryjnych • Egzamin realizowany jest w formie testu. Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń laboratoryjnych. Warunkiem koniecznym zaliczenia egzaminu jest uzyskanie z testu przynajmniej 50% możliwych do zdobycia punktów. Studentom, którzy uzyskają takie minimum przysługuje dodatkowa premia punktowa za przynajmniej dobrą ocenę uzyskaną na zaliczeniu ćwiczeń laboratoryjnych • Zarówno dla zaliczenia ćwiczeń laboratoryjnych jak i egzaminu stosowana jest następująca reguła wystawiania ocen: ocena dst: minimum 50 % możliwych do uzyskania punktów, ocena dst+: minimum 60 % możliwych do uzyskania punktów, ocena db: minimum 70 % możliwych do uzyskania punktów, ocena db+: minimum 80 % możliwych do uzyskania punktów, ocena bdb: minimum 90 % możliwych do uzyskania punktów. • Efekty W1 i W2 sprawdzane są za pomocą testu egzaminacyjnego i testów bieżących. Efekty U1 i U2 sprawdzane są za pomocą sprawozdań z ćwiczeń laboratoryjnych.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 6			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	18	0.5	
	Udział w laboratoriach	26	1	
	Udział w ćwiczeniach	0	0	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	18	0.5	
	Samodzielne przygotowanie do laboratoriów	36	1	
	Samodzielne przygotowanie do ćwiczeń			
	Samodzielna realizacja projektu			
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach	1	0	
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia	3	0	
	Udział w egzaminie / kolokwium	1	0	
	Sumaryczne obciążenie pracą studenta	103	3	
	Zajęcia z udziałem nauczycieli	46	1.5	
	Zajęcia powiązane z działalnością naukową	98	3	
Zajęcia o charakterze praktycznym	62	2		

autor

kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot

mgr inż. Łukasz Laszko

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr inż. Malinowski Tomasz

tytuł, stopień naukowy, imię, NAZWISKO, podpis