

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność		Administrator sieci komputerowych	
Semestr	VI	Program studiów, dla którego obowiązuje sylabus	2024/2025
Stopień studiów	I		

Nazwa przedmiotu	Bezpieczeństwo usług sieciowych			
Kod przedmiotu	BUS			
Łączna liczba godzin	18	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	2			

Prowadzący zajęcia	
Forma prowadzonych zajęć	Laboratorium
Wymiar zajęć	18 h
Stopień (tytuł) naukowy	
Imię	
Nazwisko	

Wymagania wstępne	Podstawowa wiedza z zakresu informatyki i technologii informacyjnych, umiejętność obsługi systemów operacyjnych Windows i Linux, znajomość podstaw programowania i algorytmiki oraz podstawowych zasad działania sieci komputerowych.
Założenia i cele przedmiotu	Celem jest przygotowanie studentów do tworzenia i utrzymania bezpiecznych środowisk sieciowych, wdrażania mechanizmów ochrony, monitorowania zagrożeń oraz reagowania na incydenty bezpieczeństwa.
Metody dydaktyczne	<ol style="list-style-type: none"> 1. Prezentacje multimedialne. 2. Pokazy przykładowych rozwiązań problemów. 3. Rozwiązywanie zadań praktycznych.

Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)		Odniesienie do efektów dla kierunku	Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji
WIEDZA – absolwent zna i rozumie:	<p>W01. Zaawansowaną wiedzę o urządzeniach i protokołach sieciowych, w tym aspektach związanych z bezpieczeństwem.</p> <p>W02. Metody projektowania systemów informatycznych z uwzględnieniem wymagań bezpieczeństwa.</p>	<p>K_W04</p> <p>K_W06</p> <p>K_W08</p> <p>K_W16</p> <p>K_W19</p>	<p>P6S_WG</p> <p>P6S_WG_INŻ</p>

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	<p>W03. Metody sztucznej inteligencji stosowane w detekcji zagrożeń i analizie anomalii w ruchu sieciowym.</p> <p>W04. Sposoby nadzorowania, zabezpieczania i obsługi sieci komputerowych w celu ochrony usług.</p> <p>W05. Koncepcje i usługi dostępne w środowiskach chmurowych, wspierające bezpieczeństwo.</p>		
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Pozyskiwać informacje z dokumentacji i raportów dotyczących bezpieczeństwa sieciowego.</p> <p>U02. Formułować i testować hipotezy dotyczące źródeł zagrożeń sieciowych.</p> <p>U03. Proponować ulepszenia w istniejących rozwiązaniach bezpieczeństwa sieciowego.</p> <p>U04. Zarządzać sieciami komputerowymi, wdrażać środki ochrony i reagować na incydenty.</p> <p>U05. Administrować systemami komputerowymi, definiować polityki bezpieczeństwa i kontrolować dostęp.</p>	K_U01 K_U02 K_U03 K_U04 K_U13 K_U17 K_U18 K_U21	P6S_UW P6S_UW_INŻ P6S_UO P6S_KK P6S_UK
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	<p>K01. Pracy w zespole, przyjmując w nim różne role.</p> <p>K02. Krytycznej oceny możliwości urządzeń sieciowych i systemów i dostępnych na rynku IT.</p> <p>K03. Ciągłego samokształcenia się w celu dostosowywania się do dynamicznie zmieniających się technologii.</p>	K_K04 K_K05 K_K06	P6S_UO P6S_KR P6S_KK

Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – laboratorium		
1	Zasady bezpieczeństwa sieciowego. Koncepcje CIA (Confidentiality, Integrity, Availability).	2
2	Zabezpieczanie usług sieciowych. HTTPS, VPN, SSH, Ipsec.	4
3	Firewall i systemy IDS/IPS. Konfiguracja, analiza logów.	4
4	Polityki bezpieczeństwa i zarządzanie ryzykiem. Tworzenie polityk, audyty bezpieczeństwa.	4
5	Ataki sieciowe i ochrona. Symulacje ataków typu DoS, spoofing, ochrona. Zaliczenie.	4

Forma i warunki zaliczenia przedmiotu	Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów.	
Metody weryfikacji efektów		Nr efektu uczenia się

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

Forma i warunki zaliczenia przedmiotu	Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów.	
uczenia się		z sylabusu
	Ocena projektów i cząstkowych prezentacji.	W01-W05, U01-U05, K01-K03

Literatura podstawowa	<ol style="list-style-type: none"> 1. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017. 2. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008. 3. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012. 4. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 5. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005.
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. S. A. Tanenbaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006. 2. B. Dunsmore, T. Skandier, <i>Cisco, technologie telekomunikacyjne</i>, MIKOM, Warszawa 2008.

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	18
Przygotowanie się do zajęć	9
Studiowanie literatury	9
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	22
Przygotowanie się do egzaminu / zaliczenia	-
Inne	-
ŁĄCZNY nakład pracy studenta w godz.	60
Liczba punktów ECTS	2