

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność		Bezpieczeństwo systemów komputerowych	
Semestr	IV	Program studiów, dla którego obowiązuje sylabus	2024/2025
Stopień studiów	I		

Nazwa przedmiotu	Zaawansowane metody sieciowe			
Kod przedmiotu	ZMS			
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	Przedmiot ma na celu zdobycie przez studentów zaawansowanej wiedzy i umiejętności w obszarze nowoczesnych technologii sieciowych, w tym protokołów routingu oraz ich zabezpieczeń, architektury sieci definiowanych programowo, wirtualizacji i segmentacji sieci, a także metod analizy ruchu, wykrywania anomalii oraz stosowania protokołów chroniących komunikację. Studenci nauczą się oceniać, projektować, konfigurować i zabezpieczać złożone infrastruktury sieciowe.
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	W01. Zaawansowane protokoły routingu (OSPF, BGP) oraz mechanizmy ich zabezpieczania.	K_W04	P6S_WG P6S_WG_INŻ

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

rozumie:	<p>W02. Koncepcję sieci definiowanych programowo (SDN), rolę kontrolerów oraz ich zastosowania w bezpieczeństwie sieci.</p> <p>W03. Metody wirtualizacji i segmentacji sieci (VLAN, VPN, mikrosegmentacja) oraz ich wpływ na bezpieczeństwo infrastruktury.</p> <p>W04. Narzędzia oraz techniki analizy ruchu sieciowego, a także rolę systemów IDS/IPS w detekcji anomalii.</p> <p>W05. Protokoły zabezpieczające komunikację (SSL/TLS, IPsec, SSH) oraz zasady ich wdrażania.</p>	<p>K_W16 K_W19</p>	
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Konfigurować i optymalizować protokoły routingu (OSPF, BGP) z uwzględnieniem zabezpieczeń.</p> <p>U02. Wdrażać i zarządzać środowiskiem SDN, w tym instalować kontrolery oraz monitorować i zabezpieczać ruch sieciowy.</p> <p>U03. Projektować i wdrażać rozwiązania wirtualizacji sieci (VLAN, VPN) oraz stosować mikrosegmentację w celu poprawy bezpieczeństwa.</p> <p>U04. Wykorzystywać narzędzia do analizy ruchu sieciowego i identyfikowania anomalii oraz wdrażać środki zaradcze z użyciem IDS/IPS.</p> <p>U05. Implementować i konfigurować protokoły takie jak SSL/TLS, IPsec i SSH, dostosowując je do wymagań sieci.</p>	<p>K_U01 K_U02 K_U03 K_U04 K_U12 K_U18 K_U21</p>	<p>P6S_UW P6S_UW_INŻ P6S_UO P6S_KK P6S_UK</p>
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>	<p>K_K04 K_K05 K_K06</p>	<p>P6S_UO P6S_KR P6S_KK</p>

Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – laboratorium		
1	Protokoły routingu i ich zabezpieczenia. OSPF, BGP; metody ochrony przed atakami na protokoły routingu.	2
2	Sieci definiowane programowo (SDN). Architektura SDN, kontrolery, zastosowania w bezpieczeństwie sieci.	4

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

3	Wirtualizacja sieci i segmentacja. Technologie VLAN, VPN; mikrosegmentacja dla zwiększenia bezpieczeństwa.	4
4	Analiza ruchu sieciowego i wykrywanie anomalii. Narzędzia i techniki monitorowania sieci; systemy IDS/IPS.	4
5	Protokoły zabezpieczające komunikację. Implementacja i konfiguracja SSL/TLS, IPsec, SSH. Zaliczenie.	4

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