

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

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

Nazwa przedmiotu	Trendy w sieciach IP			
Kod przedmiotu	TWSI			
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 zapoznanie z najnowszymi trendami w dziedzinie sieci IP: wdrożeniem IPv6, protokołami IoT, zagadnieniami bezpieczeństwa w sieciach 5G, chmurą obliczeniową i wirtualizacją funkcji sieciowych (NFV), a także automatyzacją i orkiestracją sieci z wykorzystaniem AI/ML. Studenci poznają również wpływ Internetu Rzeczy (IoT) na architekturę i bezpieczeństwo sieci IP.
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:	W01. Zna i rozumie nowe protokoły i standardy sieciowe, w tym IPv6 oraz protokoły dedykowane IoT. W02. Charakterystykę i wyzwania związane z	K_W08 K_W09 K_W16	P6S_WG P6S_WG_INŻ

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	<p>bezpieczeństwem sieci 5G.</p> <p>W03. Koncepcje chmury obliczeniowej i wirtualizacji funkcji sieciowych (NFV), a także ich wpływ na bezpieczeństwo.</p> <p>W04. Metody automatyzacji oraz orkiestracji sieci z wykorzystaniem AI/ML.</p> <p>W05. Wpływ rozwoju IoT na skalę, architekturę i bezpieczeństwo sieci IP.</p>	<p>K_W19</p> <p>K_W23</p>	
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Wdrażać i konfigurować środowiska korzystające z IPv6 oraz protokołów IoT.</p> <p>U02. Ocenic poziom bezpieczeństwa sieci 5G i zaproponować skuteczne strategie jego zwiększenia.</p> <p>U03. Wdrażać i zarządzać rozwiązaniami chmurowymi oraz NFV, dbając o ich bezpieczeństwo i optymalną konfigurację.</p> <p>U04. Zastosować narzędzia oraz techniki automatyzacji i orkiestracji sieci, wykorzystując AI/ML do wykrywania i neutralizowania zagrożeń.</p> <p>U05. Analizować wpływ wdrożenia IoT na architekturę sieci IP i proponować środki zabezpieczające oraz strategie zarządzania rosnącą liczbą urządzeń IoT.</p>	<p>K_U01</p> <p>K_U02</p> <p>K_U03</p> <p>K_U04</p> <p>K_U12</p> <p>K_U18</p> <p>K_U21</p> <p>K_U24</p> <p>K_U25</p>	<p>P6S_UW</p> <p>P6S_UW_INŻ</p> <p>P6S_UO</p> <p>P6S_KK</p> <p>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</p> <p>K_K05</p> <p>K_K06</p>	<p>P6S_UO</p> <p>P6S_KR</p> <p>P6S_KK</p>

Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – laboratorium		
1	Nowe protokoły i standardy. IPv6; protokoły dla IoT; rozwój protokołów bezpieczeństwa.	2
2	Sieci 5G i ich wpływ na bezpieczeństwo. Charakterystyka sieci 5G; wyzwania bezpieczeństwa.	4
3	Chmura obliczeniowa i wirtualizacja sieci (NFV). Bezpieczeństwo w środowiskach chmurowych; Network Function Virtualization.	4
4	Automatyzacja i orkiestracja sieci. Wykorzystanie AI/ML w zarządzaniu sieciami;	4

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	automatyczne wykrywanie i reagowanie na zagrożenia.	
5	Internet Rzeczy (IoT) i jego wpływ na sieci IP. Bezpieczeństwo urządzeń IoT; skala i zarządzanie sieciami z urządzeniami IoT. 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 sylabusa
	Ocena projektów i częściowych prezentacji.	W01-W05, U01-U05, K01-K03

Literatura podstawowa	<ol style="list-style-type: none"> 1. D. Guinard, V. Trifa, <i>Internet rzeczy</i>, Helion, Gliwice 2017. 2. M. Kief, <i>Infrastruktura jako kod. Dynamiczne systemy w epoce chmury</i>, APN Promise 2021. 3. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017. 4. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008. 5. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012. 6. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 7. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005.
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. C. Dotson, <i>Bezpieczeństwo w chmurze</i>, Helion, Gliwice 2020. 2. S. A. Tanenbaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006. 3. 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