

**WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ**

**KARTA OPISU PRZEDMIOTU**

<b>Wydział</b>	<b>Informatyki</b>		
<b>Kierunek</b>	<b>Informatyka</b>		
<b>Specjalność</b>	<b>Bezpieczeństwo systemów komputerowych Cyberbezpieczeństwo</b>		
<b>Semestr</b>	<b>IV</b>	<b>Program studiów,</b>	<b>2023/2024</b>
<b>Stopień studiów</b>	<b>I</b>	<b>dla którego obowiązuje</b>	
		<b>syllabus</b>	

<b>Nazwa przedmiotu</b>	<b>Optymalne projektowanie sieci teleinformatycznych</b>			
<b>Kod przedmiotu</b>	<b>OPST</b>			
<b>Łączna liczba godzin</b>	30	<b>Tryb</b>	stacjonarny	niestacjonarny
<b>Profil kształcenia</b>	Ogólnoakademicki (A)		Praktyczny (P)	
<b>Forma zajęć</b>	laboratorium			
<b>Język przedmiotu</b>	polski			
<b>Liczba punktów ECTS</b>	2			

<b>Prowadzący zajęcia</b>	
<b>Forma prowadzonych zajęć</b>	<b>Laboratorium</b>
<b>Wymiar zajęć</b>	<b>30 h</b>
<b>Stopień (tytuł) naukowy</b>	
<b>Imię</b>	
<b>Nazwisko</b>	

<b>Wymagania wstępne</b>	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.
<b>Założenia i cele przedmiotu</b>	Przedmiot pozwala studentom nabyć umiejętności w zakresie projektowania bezpiecznych i wydajnych sieci teleinformatycznych, w tym analizy potrzeb, doboru urządzeń i technologii, wykorzystania narzędzi symulacyjnych, optymalizacji pod kątem QoS oraz tworzenia dokumentacji zgodnej ze standardami. Studenci nauczą się efektywnie planować topologie, segmentację i warstwy zabezpieczeń, a także oceniać różne warianty architektury sieci.
<b>Metody dydaktyczne</b>	<ol style="list-style-type: none"> <li>1. Prezentacje multimedialne.</li> <li>2. Pokazy przykładowych rozwiązań problemów.</li> <li>3. Rozwiązywanie zadań praktycznych.</li> </ol>

<b>Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)</b>		<b>Odniesienie do efektów dla kierunku</b>	<b>Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji</b>
<b>WIEDZA</b> – absolwent zna i	W01. Zasady projektowania bezpiecznych sieci, obejmujące topologie, segmentację oraz	K_W04	P6S_WG P6S_WG_INŻ

## WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

rozumie:	<p>wielowarstwowe zabezpieczenia.</p> <p>W02. Kryteria doboru urządzeń i technologii sieciowych wynikające z potrzeb biznesowych oraz technicznych.</p> <p>W03. Techniki modelowania i symulacji sieci z wykorzystaniem narzędzi takich jak GNS3 czy Cisco Packet Tracer.</p> <p>W04. Metody optymalizacji wydajności sieci, w tym zarządzania przepustowością i QoS.</p> <p>W05. Znaczenie dokumentacji projektowej oraz obowiązujących standardów i norm branżowych.</p>	<p>K_W16</p> <p>K_W22</p>	
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Przygotować projekt bezpiecznej sieci, uwzględniający segmentację i warstwowe mechanizmy ochrony.</p> <p>U02. Dokonać analizy potrzeb oraz dokonać optymalnego wyboru urządzeń i technologii sieciowych.</p> <p>U03. Wykorzystać narzędzia do modelowania i symulacji w celu weryfikacji funkcjonalności i wydajności projektowanego rozwiązania.</p> <p>U04. Wdrożyć mechanizmy QoS i zarządzania przepustowością celem poprawy efektywności sieci.</p> <p>U05. Sporządzać pełną dokumentację projektową i zapewnić jej zgodność ze standardami branżowymi.</p>	<p>K_U01</p> <p>K_U02</p> <p>K_U03</p> <p>K_U04</p> <p>K_U08</p> <p>K_U13</p> <p>K_U18</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
<b>Forma zajęć – laboratorium</b>		
1	Zasady projektowania bezpiecznych sieci. Topologie sieciowe, segmentacja, warstwy zabezpieczeń.	6
2	Dobór urządzeń i technologii sieciowych. Analiza potrzeb, kryteria wyboru sprzętu i oprogramowania.	6
3	Modelowanie i symulacja sieci. Wykorzystanie narzędzi do projektowania i symulacji	6

## WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

	(np. GNS3, Cisco Packet Tracer).	
4	Optymalizacja wydajności sieci. QoS, zarządzanie przepustowością, minimalizacja opóźnień.	6
5	Dokumentacja i standardy projektowe. Tworzenie dokumentacji projektowej, zgodność ze standardami i normami. Zaliczenie.	6

<b>Forma i warunki zaliczenia przedmiotu</b>	Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów.	
<b>Metody weryfikacji efektów uczenia się</b>		<b>Nr efektu uczenia się z sylabusu</b>
	Ocena projektów i częściowych prezentacji.	W01-W05, U01-U05, K01-K03

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

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	30
Przygotowanie się do zajęć	5
Studiowanie literatury	5
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	18
Przygotowanie się do egzaminu / zaliczenia	-
Inne	-
<b>ŁĄCZNY nakład pracy studenta w godz.</b>	<b>60</b>
<b>Liczba punktów ECTS</b>	<b>2</b>