

KARTA KURSU

Nazwa	Sieci komputerowe
Nazwa w j. ang.	Computer networks

Koordynator	dr Mariusz Wojciechowski	Zespół dydaktyczny
		mgr Alfred Budziak mgr inż. Krystian Kurnik dr inż. Grzegorz Sokal dr Mariusz Wojciechowski
Punktacja ECTS*	st. stacjonarne: 5 st. niestacjonarne: 5	

Opis kursu (cele kształcenia)

Celem przedmiotu jest zapoznanie studentów z rodzajami sieci komputerowych, ich topologią oraz podstawowymi protokołami sieciowym, takimi jak na przykład: Ethernet, TCP/IP, UDP. Realizacja przedmiotu umożliwi studentom zrozumienie zasad funkcjonowania współczesnych sieci komputerowych i da podstawy teoretyczne do samodzielnego projektowania sieci.
Kurs jest realizowany w języku polskim.

Warunki wstępne

Wiedza	Znajomość teorii kodowania i metod zabezpieczania kodów, reguła parzystości. Wiedza na temat sposobów przepływu informacji w systemie operacyjnym.
Umiejętności	Kodowanie w systemie binarnym, wykonywanie obliczeń arytmetyczno-logicznych w systemie binarnym.
Kursy	Organizacja i architektura komputerów

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	W01: Ma wiedzę z przedmiotów ścisłych, zwłaszcza matematyki i fizyki, niezbędną do opisu i analizy działania sieci komputerowych i urządzeń sieciowych, a także innych urządzeń zakresu technik komputerowych oraz algorytmów ich funkcjonowania.	K_W01 K_W09 K_W12 K_W13 K_W14

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	U01: Potrafi korzystać z nowoczesnych narzędzi TI w zakresie planowania, budowania i eksploatacji sieci komputerowych o lokalnym i rozszerzonym zasięgu w oparciu o zasady bezpieczeństwa funkcjonowania tych struktur. U02: Potrafi analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania.	K_U01 K_U07 K_U08 K_U09 K_U16 K_U17

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student:	
	K01: Rozumie istotę pracy zespołowej, współdziałania z innymi osobami w ramach prac zespołowych i podejmowania różnych wiodących ról w interdyscyplinarnych zespołach oraz znaczenie konstruktywnej dyskusji w rozwiązywaniu problemów w obszarze bezpieczeństwa.	K_K01 K_K02 K_K03 K_K05

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	30					30					

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	15					20					

Opis metod prowadzenia zajęć

Zajęcia praktyczne łączą **laboratoria, projekty, symulacje oraz analizę przypadków**, aby zapewnić studentom realne doświadczenie w konfiguracji, zarządzaniu i zabezpieczaniu infrastruktury sieciowej.

- ♦ **Ćwiczenia laboratoryjne** – studenci pracują z rzeczywistym sprzętem i symulatorami, konfiguruje sieci i implementując mechanizmy bezpieczeństwa.
- ♦ **Metoda projektowa** – realizacja indywidualnych i zespołowych projektów, rozwijających umiejętność planowania i wdrażania sieci.

- ♦ **Studia przypadków i scenariusze problemowe** – analiza rzeczywistych incydentów, diagnozowanie problemów i wdrażanie rozwiązań.
- ♦ **Symulacje i testowanie konfiguracji** – praca w wirtualnych środowiskach, umożliwiającą eksperymentowanie i optymalizację systemów.
- ♦ **Warsztaty i współpraca zespołowa** – interaktywne zajęcia, podczas których studenci wspólnie rozwiązują problemy i uczą się pracy w grupie.
- ♦ **Odwrócona klasa i samodzielna analiza** – przygotowanie przed zajęciami umożliwia efektywne wykorzystanie czasu na praktykę i dyskusję.
- ♦ **Bieżąca ewaluacja i feedback** – ocena postępów poprzez testy, zadania kontrolne oraz prezentacje projektów.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					X	X		X					
U01					X	X		X					
U02					X	X		X					
K01					X	X		X					

Kryteria oceny	Zaliczenie kursu opiera się na ocenie efektów kształcenia osiągniętych przez studenta w ramach pracy indywidualnej lub zespołowej. Warunkiem uzyskania zaliczenia jest spełnienie następujących wymagań: 1. Projekt zaliczeniowy lub ćwiczenia praktyczne - Student wykonuje projekt zaliczeniowy zgodnie z wytycznymi prowadzącego lub realizuje zadania praktyczne podczas zajęć. - Forma zaliczenia może obejmować zarówno samodzielnie wykonany projekt, jak i praktyczne ćwiczenia laboratoryjne, w zależności od specyfiki grupy i ustaleń prowadzącego. 2. Test teoretyczny - Weryfikacja wiedzy teoretycznej odbywa się poprzez test zaliczeniowy lub serię krótszych testów częściowych. - Warunkiem zaliczenia jest uzyskanie co najmniej 50% punktów z testu. 3. Certyfikat Cisco Networking Academy - Student zobowiązany jest do ukończenia oraz przesłania wskazanego przez prowadzącego certyfikatu uzyskanego w ramach lokalnej akademii Cisco. Zaliczenie kursu jest uzależnione od spełnienia tego warunku, a brak przesłania certyfikatu skutkuje brakiem możliwości zaliczenia kursu. Aby uzyskać zaliczenie kursu, student musi spełnić wszystkie trzy warunki: ✅ Pomyślnie ukończyć projekt lub ćwiczenie laboratoryjne, ✅ Uzyskać wymagany wynik z testu teoretycznego, ✅ Przedstawić ukończony certyfikat Cisco Networking Academy, Szczegółowe wymagania dotyczące formy realizacji projektu, zakresu testów oraz uzyskania certyfikatu są określone przez prowadzącego.
----------------	--

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

Na tym poziomie studenci przechodzą do rzeczywistej konfiguracji sieci z wykorzystaniem routerów i switchy MikroTik. W pełni praktyczne zajęcia obejmują wdrażanie protokołów, konfigurację VLAN-ów oraz zabezpieczeń na urządzeniach MikroTik.

1. Wprowadzenie do systemu RouterOS i interfejsu WinBox

- Omówienie systemu RouterOS
- Pierwsza konfiguracja routera MikroTik
- Zarządzanie interfejsem CLI i GUI

2. Konfiguracja VLAN-ów i routingu dynamicznego

- Implementacja VLAN-ów na MikroTik (switching i routing VLAN)
- Routing dynamiczny w RouterOS: OSPF, RIP
- Optymalizacja i zabezpieczanie protokołów routingu

3. Zabezpieczenia na MikroTik

- Ochrona urządzeń MikroTik (hasła, dostęp, użytkownicy)
- Firewall i filtrowanie ruchu – podstawy zabezpieczeń w RouterOS
- Wykorzystanie list adresowych (Address Lists) do zarządzania dostępem
- Ochrona przed atakami DDoS i innymi zagrożeniami

4. Implementacja VPN w RouterOS

- Wprowadzenie do tunelowania i protokołów VPN (PPTP, L2TP/IPSec, OpenVPN)
- Konfiguracja połączeń VPN w RouterOS
- Zabezpieczenia i monitorowanie ruchu VPN

Laboratoria: Wszystkie konfiguracje realizowane są na rzeczywistych urządzeniach MikroTik w warunkach laboratoryjnych.

Wykaz literatury podstawowej

Łukasz Guziak – *Konfiguracja usług sieciowych na urządzeniach MikroTik*, Helion, 2024.

Praktyczny przewodnik po konfiguracji usług sieciowych z wykorzystaniem urządzeń MikroTik.

Marek Serafin – *Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone*, Helion, 2020.

Omówienie implementacji sieci VPN z uwzględnieniem urządzeń MikroTik.

Piotr Jabłoński – *MikroTik RouterOS. Praktyczne zastosowania*, Helion, 2019.

Przewodnik po praktycznych zastosowaniach systemu RouterOS w sieciach komputerowych.

Tomasz Dąg – *MikroTik w praktyce. Rozwiązania dla domu i biura*, Helion, 2021.

Książka przedstawia praktyczne scenariusze wykorzystania urządzeń MikroTik w różnych środowiskach.

Łukasz Bromirski – *MikroTik dla profesjonalistów*, Helion, 2019.

Zaawansowane techniki konfiguracji i zarządzania urządzeniami MikroTik.

Paweł Józwiak – *MikroTik. Przewodnik dla administratora sieci*, Helion, 2020.

Kompleksowy przewodnik dla administratorów sieci wykorzystujących urządzenia MikroTik.

Krzysztof Kuczyński – *MikroTik RouterOS. Zaawansowana konfiguracja i zabezpieczenia*, Helion, 2021.

Omówienie zaawansowanych technik konfiguracji i zabezpieczeń w RouterOS.

Marcin Bury – *MikroTik. Sztuka konfiguracji*, Helion, 2022.

Praktyczne podejście do konfiguracji urządzeń MikroTik w różnych scenariuszach sieciowych.

Andrzej Karpiński – *MikroTik RouterOS. Przewodnik po systemie*, Helion, 2020.

Szczegółowy przewodnik po systemie RouterOS, jego funkcjach i możliwościach.

Łukasz Guziak – *Konfiguracja usług sieciowych na urządzeniach MikroTik. Bezpieczeństwo sieci*, Helion, 2024.

Skupienie na aspektach bezpieczeństwa przy konfiguracji usług sieciowych na urządzeniach MikroTik.

Wykaz literatury uzupełniającej

Marek Serafin – *Bezpieczeństwo sieci firmowej. Kontrola ruchu wychodzącego*, Helion, 2020.

Analiza metod kontroli ruchu sieciowego z uwzględnieniem urządzeń MikroTik.

Piotr Jabłoński – *RouterOS. Praktyczne przykłady konfiguracji*, Helion, 2018.

Zbiór praktycznych przykładów konfiguracji systemu RouterOS.

Tomasz Drąg – *MikroTik w małej firmie. Praktyczne wdrożenia*, Helion, 2021.

Przewodnik po wdrożeniach urządzeń MikroTik w środowiskach małych firm.

Łukasz Bromirski – *Sieci komputerowe. Kompendium wiedzy*, Helion, 2017.

Kompleksowe omówienie zagadnień sieciowych z uwzględnieniem różnych urządzeń, w tym MikroTik.

Paweł Józwiak – *Firewall w RouterOS. Ochrona sieci z MikroTik*, Helion, 2020.

Szczegółowe omówienie konfiguracji firewalla w systemie RouterOS.

Krzysztof Kuczyński – *QoS w sieciach opartych na MikroTik*, Helion, 2021.

Zarządzanie jakością usług w sieciach z wykorzystaniem urządzeń MikroTik.

Marcin Bury – *MikroTik. Rozwiązania dla ISP*, Helion, 2022.

Specjalistyczne rozwiązania dla dostawców usług internetowych z użyciem MikroTik.

Andrzej Karpiński – *VPN w RouterOS. Bezpieczne połączenia z MikroTik*, Helion, 2020.

Implementacja i zarządzanie sieciami VPN w systemie RouterOS.

Łukasz Guziak – *MikroTik. Praktyczne aspekty bezpieczeństwa*, Helion, 2024.

Praktyczne podejście do zabezpieczania sieci z wykorzystaniem urządzeń MikroTik.

Marek Serafin – *Wirtualizacja w praktyce*, Helion, 2019.

Omówienie zagadnień wirtualizacji z uwzględnieniem konfiguracji sieci w środowiskach wirtualnych.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – studia stacjonarne

Liczba godzin w kontakcie z prowadzącymi	Wykład	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	0
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		110

Liczba punktów ECTS w zależności od przyjętego przelicznika	5
---	---

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	0
	Przygotowanie do egzaminu/zaliczenia	25
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		5