

KARTA KURSU

Nazwa	Bezpieczeństwo sieci komputerowych 2
Nazwa w j. ang.	Security of computer networks 2

Koordynator	dr Mariusz Wojciechowski	Zespół dydaktyczny
		mgr Alfred Budziak mgr inż. Krystian Kurnik dr inż. Grzegorz Sokal dr Mariusz Wojciechowski
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

Kurs koncentruje się na zaawansowanych aspektach ochrony infrastruktury sieciowej, obejmujących zarówno strategię defensywną, jak i metody analizy incydentów bezpieczeństwa. Studenci zdobędą umiejętności konfigurowania i zarządzania mechanizmami zabezpieczeń na poziomie sieci lokalnych (LAN), rozległych (WAN) oraz środowisk chmurowych i hybrydowych.

Zajęcia obejmują praktyczną konfigurację systemów firewall (Cisco, MikroTik, pfSense), list kontroli dostępu (ACL), systemów wykrywania i zapobiegania włamaniom (IDS/IPS), a także wdrażanie polityk uwierzytelniania i kontroli dostępu z wykorzystaniem RADIUS oraz TACACS+. Kurs kładzie nacisk na analizę ruchu sieciowego pod kątem wykrywania zagrożeń oraz implementację systemów VPN zapewniających bezpieczną transmisję danych.

Dodatkowo, studenci poznają techniki przeprowadzania testów penetracyjnych, identyfikowania podatności sieci oraz stosowania zasad **Zero Trust Security** w nowoczesnych organizacjach. Kurs przygotowuje uczestników do pracy jako specjaliści ds. bezpieczeństwa sieci w korporacjach, administracji publicznej oraz sektorze IT.

Kurs realizowany jest w formie wykładów w języku polskim oraz intensywnych laboratoriów, podczas których uczestnicy będą implementować rzeczywiste rozwiązania na urządzeniach sieciowych oraz analizować rzeczywiste przypadki ataków i naruszeń bezpieczeństwa.

Warunki wstępne

Wiedza	Znajomość modelu ISO/OSI oraz funkcji poszczególnych warstw oraz protokołów. Znajomość podstawowych mechanizmów zabezpieczania sieci (ACL, VLAN, podstawy firewalli). Zrozumienie podstaw kryptografii oraz metod szyfrowania stosowanych w transmisji danych (SSL/TLS, IPSec).
Umiejętności	Umiejętność konfiguracji podstawowych usług sieciowych (DHCP, DNS, NAT). Implementacja routingu statycznego i dynamicznego na urządzeniach Cisco i MikroTik. Integracja usług sieciowych i administracja politykami dostępu. Umiejętność konfigurowania urządzeń sieciowych w CLI oraz stosowania podstawowych metod zarządzania bezpieczeństwem.
Kursy	Podstawy bezpieczeństwa sieci komputerowych – znajomość zagrożeń, firewalli oraz technik ataku i obrony. Sieci komputerowe – zasady routingu i przełączania, konfiguracja urządzeń. Administracja systemami operacyjnymi – konfiguracja systemów i usług sieciowych pod kątem bezpieczeństwa.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	<p>W01: Ma wiedzę w zakresie zabezpieczania architektury systemów komputerowych i urządzeń sieciowych w lokalnych i rozległych sieciach komputerowych.</p> <p>W02: Zna i rozumie zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji.</p>	<p>K_W04 K_W02 K_W07</p>

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	<p>U01: Potrafi opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania lub projektu, w szczególności związanych z bezpieczeństwem teleinformatycznym.</p> <p>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.</p> <p>U03: Potrafi konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych.</p>	<p>K_U01 K_U05 K_U06 K_U07 K_U08 K_U09 K_U10</p>

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student:	
	<p>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 cyberbezpieczeństwa.</p>	<p>K_K01 K_K02 K_K03 K_K05</p>

Studia stacjonarne

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

Studia niestacjonarne

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

Zajęcia kładą nacisk na **praktyczne zastosowanie wiedzy, rozwiązywanie problemów oraz rozwój umiejętności analitycznych i zespołowych**, przygotowując studentów do pracy w rzeczywistych środowiskach sieciowych i bezpieczeństwa IT.

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	X					
W02					X	X	X	X					
U01					X	X	X	X					
U02					X	X	X	X					
U03					X	X	X	X					
K01					X	X	X	X					

Kryteria oceny	<p>Zaliczenie kursu opiera się na ocenie efektów kształcenia osiągniętych przez studenta w ramach pracy indywidualnej lub zespołowej. Warunkiem uzyskania zaliczenia jest spełnienie następujących wymagań:</p> <ol style="list-style-type: none"> 1. Projekt zaliczeniowy lub ćwiczenia praktyczne <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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
----------------	---

	<p>przesłania certyfikatu skutkuje brakiem możliwości zaliczenia kursu.</p> <p>Aby uzyskać zaliczenie kursu, student musi spełnić wszystkie trzy warunki:</p> <ul style="list-style-type: none"> ✓ Pomyślnie ukończyć projekt lub ćwiczenie laboratoryjne, ✓ Uzyskać wymagany wynik z testu teoretycznego, ✓ Przedstawić ukończony certyfikat Cisco Networking Academy, <p>Szczegółowe wymagania dotyczące formy realizacji projektu, zakresu testów oraz uzyskania certyfikatu są określone przez prowadzącego.</p>
Uwagi	

Treści merytoryczne (wykaz tematów)

Ostatni poziom skupia się wyłącznie na bezpieczeństwie sieci i urządzeń, zarówno w środowisku Cisco, jak i MikroTik. Studenci poznają metody ochrony przed cyberatakami, analizę ruchu oraz strategie wykrywania i minimalizowania zagrożeń.

1. Zaawansowane mechanizmy zabezpieczeń sieciowych (Cisco & MikroTik)

- Ochrona dostępu do sieci: 802.1X, RADIUS, TACACS+
- Rozszerzone listy ACL i kontrola dostępu do usług
- Filtracja ruchu na podstawie Deep Packet Inspection (DPI)

2. Wykrywanie i reagowanie na ataki

- Ataki na sieci VLAN i sposoby ich zapobiegania
- IDS/IPS – Intrusion Detection and Prevention Systems
- Analiza pakietów przy użyciu Wireshark i narzędzi monitorujących

3. Segmentacja i izolacja sieci dla bezpieczeństwa

- Mikrosegmentacja sieci jako strategia ochrony
- Praktyczne wdrożenie zabezpieczeń na poziomie VLAN
- Konfiguracja DMZ dla ochrony usług publicznych

4. Zaawansowane zarządzanie VPN i szyfrowanie ruchu

- Implementacja IPSec VPN na Cisco i MikroTik
- Zabezpieczenie tuneli VPN przed atakami
- Wprowadzenie do VPN typu Site-to-Site i Remote Access

5. Implementacja VPN w RouterOS

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

6. Symulacja ataków i analiza incydentów

- Przeprowadzanie testów penetracyjnych na warstwie sieciowej
- Analiza skuteczności zabezpieczeń i testy odporności na ataki
- Tworzenie polityki bezpieczeństwa dla firmowej infrastruktury IT

Laboratoria: Konfiguracja rzeczywistych urządzeń Cisco i MikroTik oraz analiza ruchu sieciowego pod kątem bezpieczeństwa.

Wykaz literatury podstawowej

Adam Józefiok – *CCNP 350-401 ENCOR. Zaawansowane administrowanie siecią Cisco*, Helion, 2022. Kompleksowy przewodnik po zaawansowanych technikach zarządzania sieciami Cisco, przygotowujący do egzaminu CCNP ENCOR.

Łukasz Bromirski – *Bezpieczeństwo sieci komputerowych. Receptury*, Helion, 2020.

Praktyczne podejście do zabezpieczania sieci komputerowych z uwzględnieniem urządzeń Cisco i MikroTik.

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

Szczegółowe omówienie konfiguracji i zarządzania firewallem w systemie MikroTik RouterOS.

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

Analiza metod kontroli ruchu sieciowego z uwzględnieniem urządzeń Cisco i 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.
Wendell Odom – *CCNA 200-301. Oficjalny podręcznik. Część 2*, Cisco Press, 2020.
 Kontynuacja podręcznika, skupiająca się na bardziej zaawansowanych zagadnieniach sieciowych.
David Hucaby – *CCNA 200-301. Oficjalny podręcznik certyfikacyjny*, Cisco Press, 2020.
 Oficjalny podręcznik Cisco, obejmujący szeroki zakres tematów związanych z sieciami.

Wykaz literatury uzupełniającej

Chris Sanders – *Praktyczna analiza ruchu sieciowego. Wydanie II*, Helion, 2017.
 Przewodnik po analizie ruchu sieciowego z użyciem narzędzia Wireshark.
William Stallings – *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i mechanizmy*, Helion, 2011.
 Kompleksowe omówienie zagadnień związanych z kryptografią i bezpieczeństwem sieci.
Behrouz A. Forouzan – *Sieci komputerowe. Ochrona danych*, Helion, 2007.
 Podręcznik omawiający metody ochrony danych w sieciach komputerowych.
Michael W. Lucas – *Sieci komputerowe. Księga eksperta*, Helion, 2004.
 Zaawansowane techniki zarządzania i konfiguracji sieci komputerowych.
Radek Vystavěl – *Cisco. Protokoły routingu*, Helion, 2006.
 Przewodnik po protokołach routingu stosowanych w urządzeniach Cisco.
Jeff Doyle, Jennifer DeHaven Carroll – *Routing TCP/IP. Tom 1*, Cisco Press, 2005.
 Dogłębne omówienie protokołów routingu TCP/IP.
Jeff Doyle, Jennifer DeHaven Carroll – *Routing TCP/IP. Tom 2*, Cisco Press, 2001.
 Kontynuacja pierwszego tomu, skupiająca się na zaawansowanych technikach routingu.
Kevin Wallace – *CCNA Routing and Switching 200-125. Oficjalny podręcznik*, Cisco Press, 2016.
 Podręcznik omawiający zagadnienia routingu i przełączania w sieciach Cisco.
James F. Kurose, Keith W. Ross – *Sieci komputerowe. Ujęcie top-down*, Helion, 2013.
 Nowoczesne podejście do nauki sieci komputerowych, zaczynające od warstwy aplikacji.
Charles M. Kozierok – *TCP/IP. Ilustrowany przewodnik*, Helion, 2006.
 Szczegółowy przewodnik po protokołach TCP/IP z licznymi ilustracjami.

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	0
	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	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	0
	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	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3