

WSTI w Katowicach, kierunek Informatyka, stopień II
opis modułu *Bezpieczeństwo sieci rozległych i zarządzanie jakością usług w sieciach IP*
**BEZPIECZEŃSTWO SIECI ROZLEGŁYCH I ZARZĄDZANIE JAKOŚCIĄ USŁUG
W SIECIACH IP**

Kod przedmiotu: BSST-BSR2

Rodzaj przedmiotu: kierunkowy, obieralny

Specjalność: Bezpieczeństwo sieci i systemów teleinformatycznych

Wydział: Informatyki

Kierunek: Informatyka

Poziom studiów: drugiego stopnia – VII poziom PRK

Profil studiów: praktyczny

Forma studiów: stacjonarna/niestacjonarna

Rok: 1

Semestr: 2

Formy zajęć i liczba godzin:

Forma stacjonarna

wykłady – 15

laboratorium – 45

Forma niestacjonarna

wykłady – 10

laboratorium – 24

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 5

Osoby prowadzące:

wykład:

laboratorium:

1. Założenia i cele przedmiotu:

Celem przedmiotu jest przekazanie studentom wiedzy na temat wybranych zagadnień bezpieczeństwa komunikacji w ramach rozległej sieci komputerowej, w szczególności technologii takich jak wirtualne sieci prywatne, technologie filtrowania ruchu sieciowego, wysoka dostępność procesu routingu oraz Quality of Service w sieciach IP.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi:

Przedmioty wprowadzające to: Kryptograficzne metody ochrony informacji, Zaawansowany routing w sieciach TCP/IP, Bezpieczeństwo przełączanych sieci LAN oraz sieci bezprzewodowych.

3. Opis form zajęć

a) *Wykłady*

- **Treści programowe:**
 - Problematyka technologii filtrowania ruchu sieciowego,
 - Problematyka uwierzytelniania w ruterach sprzętowych,
 - Realizacja dostępu zdalnego do zasobów sieciowych firmowej sieci komputerowej z wykorzystaniem usługi VPN,
 - Wprowadzenie do Quality of Service,
 - Problematyka zawłaszczenia przepustowości łącza internetowego
 - Algorytmy przeciwdziałania przeciążeniom a algorytmy szeregowania pakietów
 - Algorytmy szeregowania pakietów wykorzystywane w realizacji podziału łącza internetowego,
 - Technologia MPLS,
 - Redundancja routerów, protokoły HSRP, VRRP oraz GLBP.

- **Metody dydaktyczne:**
 - Wykład prowadzony jest w formie prezentacji, uzupełnionej przykładami rozwiązywanymi w trakcie wykładu na tablicy oraz na rzutniku multimedialnym. W ramach wykładu, prowadzący wspólnie ze studentami omawiają praktyczne zastosowania prezentowanych treści.

- **Forma i warunki zaliczenia:**
 - Warunkiem zaliczenia wykładu jest zdanie egzaminu końcowego z przedmiotu w formie pisemnej

- **Wykaz literatury podstawowej:**
 1. Materiały multimedialne dostępne online – <http://moodle.wsti.pl>
 2. Józefiok A.: CCNA 200-301. Zostań administratorem sieci komputerowych Cisco. Gliwice: Helion, cop. 2020.
 3. Suehring S.: Zapory sieciowe w systemie Linux. Kompendium wiedzy o nftables. Wydanie IV. Wyd. Helion, Gliwice 2015
 4. Kalsi T.: Bezpieczeństwo systemu Linux w praktyce. Receptury. Gliwice: HELION, cop. 2019.
 5. Serafin M.: Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Wyd. Helion, Gliwice 2013
 6. Józefiok A.: CCNA 200-120. Zostań administratorem sieci komputerowych Cisco. Wyd. Helion, Gliwice 2015
 7. Hassan M., Raj J.: Wysoko wydajne sieci TCP/IP. Wyd. Helion, Gliwice 2004

- **Wykaz literatury uzupełniającej:**
 1. Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
 2. Rash M.: Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort. Wyd. Helion, Gliwice 2008
 3. Innokenty Rudenko, Tsunami Computing: Routery Cisco. Czarna księga. Wyd. Helion, Gliwice 2001
 4. Binnie Ch.: Linux Server. Bezpieczeństwo i ochrona sieci. Gliwice: HELION, cop. 2017.

b) Laboratorium

• **Treści programowe:**

- Wdrażanie technologii filtrowania ruchu sieciowego w ruterach Cisco (standardowe, rozszerzone, dynamiczne, refleksyjne i czasowe ACL, implementacja Context-Based Access Control (CBAC), implementacja Zone-Based Firewall (ZBF)),
- Wdrażanie systemów ochrony przed włamaniami w oparciu o routery Cisco (Cisco IOS Intrusion Prevention System (IPS)),
- Wdrażanie technologii filtrowania ruchu w ruterach opartych na systemie operacyjnym GNU/Linux z wykorzystaniem iptables,
- Wdrażanie tunelu VPN z wykorzystaniem protokołu GRE w routerach Cisco,
- Wdrażanie wirtualnych sieci prywatnych w systemie MS Windows Server (m.in. Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), Internet Key Exchange v2 (IKEv2), and Secure Socket Tunneling Protocol (SSTP), Direct Access, CMAK, zasady dostępu zdalnego w serwerze NPS),
- Instalacja i konfiguracja serwera VPN w systemie GNU/Linux (pptpd, OpenVPN),
- Wdrażanie wirtualnych sieci prywatnych na routerach Cisco (Site-to-Site IPSec VPN, client-to-site IPSec VPN, client-to-site SSL VPN),
- Badanie wpływu algorytmu FIFO na ruch sieciowy przepływający przez ruter
- Algorytmy sprawiedliwego podziału łącza w ruterach opartych na systemie operacyjnym GNU/Linux (SFQ, ESFQ, WRR),
- Algorytmy hierarchicznego podziału łącza w ruterach opartych na systemie operacyjnym GNU/Linux (HTB),
- Ograniczanie pasma za pomocą IMQ, iptables oraz Layer7 w ruterach opartych na systemie operacyjnym GNU/Linux,
- Wdrażanie MPLS VPN,
- Redundancja routerów, protokoły HSRP, VRRP oraz GLBP,
- Wdrażanie mechanizmów QoS w routerach Cisco.

• **Metody dydaktyczne:**

- W trakcie laboratorium prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń z wykorzystaniem rzutnika multimedialnego, a następnie studenci samodzielnie realizują zadania określone przez prowadzącego opisane w platformie e-learningowej Moodle.

• **Forma i warunki zaliczenia:**

- Warunkiem zaliczenia przedmiotu jest uczestnictwo studenta na zajęciach laboratoryjnych oraz wykazanie się wiedzą z zakresu programu przedmiotu. Studenci uzyskują zaliczenie poprzez zdobycie określonej ilości punktów, przyznawanych za sprawozdania realizowane w trakcie zajęć, oraz sprawozdania zrealizowane z zadań do samodzielnego wykonania w domu po każdym laboratorium, oraz zaliczenia końcowego na ostatnich zajęciach. Zaliczenie otrzymuje student, który uzyskał określoną liczbę punktów, a o której informacja jest opublikowana na stronach WSTI. Ocenę z zaliczenia student uzyskuje w skali wskazanej w regulaminie studiów.

• **Wykaz literatury podstawowej:**

1. Materiały multimedialne dostępne online – <http://moodle.wsti.pl>
2. Józefiok A.: CCNA 200-301. Zostań administratorem sieci komputerowych Cisco. Gliwice: Helion, cop. 2020.
3. Suehring S.: Zapory sieciowe w systemie Linux. Kompendium wiedzy o nftables. Wydanie IV. Wyd. Helion, Gliwice 2015
4. Kalsi T.: Bezpieczeństwo systemu Linux w praktyce. Receptury. Gliwice: HELION, cop. 2019.
5. Serafin M.: Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Wyd. Helion, Gliwice 2013
6. Józefiok A.: CCNA 200-120. Zostań administratorem sieci komputerowych Cisco. Wyd. Helion, Gliwice 2015
7. Hassan M., Raj J.: Wysoko wydajne sieci TCP/IP. Wyd. Helion, Gliwice 2004

• **Wykaz literatury uzupełniającej:**

1. Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
2. Rash M.: Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort. Wyd. Helion, Gliwice 2008
3. Innokenty Rudenko, Tsunami Computing: Routery Cisco. Czarna księga. Wyd. Helion, Gliwice 2001
4. Binnie Ch.: Linux Server. Bezpieczeństwo i ochrona sieci. Gliwice: HELION, cop. 2017.

4. Opis sposobu wyznaczania punktów ECTS

a. forma stacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	15
	Czytanie wskazanej literatury	15
	Przygotowanie do egzaminu	15
Laboratorium	Kontakt z nauczycielem	45
	Czytanie wskazanej literatury	20
	Samodzielne rozwiązywanie zadań	15

Całkowita ilość godzin aktywności studenta	125
Liczba punktów ECTS dla modułu/przedmiotu	5

b. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	10
	Czytanie wskazanej literatury	10
	Przygotowanie do egzaminu	25
Laboratorium	Kontakt z nauczycielem	25
	Czytanie wskazanej literatury	30
	Samodzielne rozwiązywanie zadań	25

Całkowita ilość godzin aktywności studenta	125
Liczba punktów ECTS dla modułu/przedmiotu	5

5. Wskaźniki sumaryczne

a. forma stacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
- Liczba godzin kontaktowych – 45
 - Liczba punktów ECTS – 1,8
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
- Liczba godzin kontaktowych – 45
 - Liczba punktów ECTS – 3,2

b. forma niestacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
- Liczba godzin kontaktowych – 35
 - Liczba punktów ECTS – 1,4
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
- Liczba godzin kontaktowych – 25
 - Liczba punktów ECTS – 3,2

6. Zakładane efekty uczenia się.

Efekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
-----------------------------	-----------------------------------	---

BSST-BSR2_01	... ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie stosowania technologii Quality of Service	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K01, IIK_K02, IIK_K04
BSST-BSR2_02	... ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie stosowania technologii wirtualnych sieci prywatnych	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K01, IIK_K02, IIK_K04
BSST-BSR2_03	... ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie stosowania technologii filtrowania ruchu sieciowego	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K01, IIK_K02, IIK_K04
BSST-BSR2_04	... ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie stosowania technologii wysokiej dostępności routerów	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K01, IIK_K02, IIK_K04

7. Odniesienie efektów uczenia się do form zajęć i sposób oceny osiągnięcia przez studenta efektów uczenia się.

Efekt przedmiotowy (Symbol)	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	Wykład	Laboratorium	
BSST-BSR2_01	v	v	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
BSST-BSR2_02	v	v	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
BSST-BSR2_03	v	v	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
BSST-BSR2_04	v	v	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się.

Efekt przedmiotowy (Symbol)	Efekt jest uznawany za osiągnięty, gdy student:

WSTI w Katowicach, kierunek Informatyka, stopień II
opis modułu ***Bezpieczeństwo sieci rozległych i zarządzanie jakością usług w sieciach IP***

BSST-BSR2_01	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
BSST-BSR2_02	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
BSST-BSR2_03	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
BSST-BSR2_04	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.