



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



SYLABUS PRZEDMIOTU

Zabezpieczenia protokołów sieciowych

I. Informacje ogólne

Nazwa przedmiotu	<i>Zabezpieczenia protokołów sieciowych</i>
Kod przedmiotu	ZPS
Rodzaj przedmiotu	Fakultatywny
Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil kształcenia	Ogólnoakademicki
Rok studiów	pierwszy
Rodzaje zajęć i liczba godzin	
Wykład	0
Ćwiczenia	0
Laboratoria	30
Praktyki	0
Liczba punktów ECTS	3

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy
(wykładowców)/ prowadzących zajęcia

- mgr Tomasz Zaworski, zawoor@wmi.amu.edu.pl

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	tak, częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- rozwój umiejętności konfiguracji urządzeń do obsługi średniej wielkości sieci lokalnej
- poszerzenie wiedzy na temat możliwych ataków na sieć komputerową

- nabycie umiejętności użycia protokołów pozwalających zabezpieczyć przesyłane informacje
- poznanie sposobów na zwiększenie stabilności i niezawodności sieci komputerowej

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Podstawy sieci komputerowych na poziomie inżyniera informatyki, język angielski w stopniu umożliwiającym biegłe posługiwanie się dokumentacją.

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
ZPS_01	KINF2_W02	Rozumie pojęcia związane z transmisją danych w sieciach komputerowych opartych o model TCP/IP.
ZPS_02	KINF2_W03	Potrafi używać wiersz poleceń systemu Cisco IOS.
ZPS_03	KINF2_W03 KINF2_U07	Potrafi użyć protokoły Telnet i SSH do zdalnego zarządzania sprzętem sieciowym oraz zna ich wady i zalety.
ZPS_04	KINF2_W03 KINF2_U07	Rozumie problemy związane z użyciem dużej liczby komputerów w jednej domenie rozgłoszeniowej i potrafi je rozwiązać stosując VLANy.
ZPS_05	KINF2_W04	Potrafi zabezpieczyć urządzenia przed atakiem zalewania adresami MAC.
ZPS_06	KINF2_W03	Zna problemy związane z użyciem Dynamic Trunking Protocol i potrafi im zapobiegać.
ZPS_07	KINF2_W04 KINF2_U04	Rozumie niebezpieczeństwo pętli w sieci komputerowej i umie konfigurować Spanning Tree Protocol.
ZPS_08	KINF2_W04	Potrafi wdrożyć redundancję łącza.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



ZPS_09	KINF2_W03 KINF2_U04	Zna pojęcie routingu w sieciach komputerowych.
ZPS_10	KINF2_W03 KINF2_U04	Potrafi użyć protokołu OSPF i zabezpieczyć go.
ZPS_11	KINF2_W03 KINF2_U04	Potrafi użyć protokołu EIGRP i zabezpieczyć go.
ZPS_12	KINF2_W04	Potrafi wdrożyć redundancję bramy sieciowej przy użyciu protokołu HSRP.
ZPS_13	KINF2_W03 KINF2_U07	Potrafi przeciwdziałać atakom związanym z protokołem DHCP.
ZPS_14	KINF2_W03 KINF2_U02	Zna metody filtrowania niepożądanego ruchu sieciowego przy użyciu list dostępu.
ZPS_15	KINF2_W03	Potrafi uruchomić szyfrowany tunel pomiędzy urządzeniami obsługującymi ruch sieciowy.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma			30	45	
1.	ZPS_01		2	3	Omówienie pojęć związanych z transmisją danych w sieciach komputerowych.
2.	ZPS_02		2	3	Zapoznanie ze sprzętem sieciowym. Podstawy obsługi systemu operacyjnego Cisco IOS.
3.	ZPS_03		2	3	Konfiguracja protokołów zdalnego zarządzania: Telnet i SSH.
4.	ZPS_04		3	6	Zagrożenia związane z dużą domeną rozgłoszeniową. Konfiguracja wirtualnej sieci lokalnej.
5.	ZPS_05		1	2	Zabezpieczanie portów przy użyciu Port Security.
6.	ZPS_06		1	2	Omówienie Dynamic Trunking Protocol i zagrożeń z nim związanych.
7.	ZPS_07		3	6	Spanning Tree Protocol jako rozwiązanie problemu przypadkowych pętli.
8.	ZPS_08		1	2	Zabezpieczanie sieci lokalnej przed awarią pojedynczego łącza.
9.	ZPS_09		1	2	Podstawy routingu.
10.	ZPS_10		3	6	Routing dynamiczny na przykładzie OSPF. Zabezpieczanie protokołu OSPF.
11.	ZPS_11		3	6	Routing dynamiczny na przykładzie EIGRP. Zabezpieczanie protokołu EIGRP.
12.	ZPS_12		2	3	Redundancja bramy sieciowej.
13.	ZPS_13		2	3	Przeciwdziałanie atakom związanym z protokołem DHCP.
14.	ZPS_14		2	3	Filtrowanie niepożądanego ruchu sieciowego przy użyciu list dostępu.
15.	ZPS_15		2	3	Szyfrowanie ruchu w tunelu sieciowym.

5. Zalecana literatura

- 1) Wendell Odom, „CCNA Routing and Switching 200-125 Official Cert Guide Library”, Cisco Press, 2016
- 2) Adam Józefiok, „CCNA 200-125. Zostań administratorem sieci komputerowych Cisco”, Wydawnictwo Helion, 2017
- 3) Andrew S. Tanenbaum, David J. Wetherall, „Sieci komputerowe. Wydanie V”, Wydawnictwo Helion, 2012

V. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
✓	Dyskusja
	Praca z tekstem
	Metoda analizy przypadków
	Uczenie problemowe (Problem-based learning)
	Gra dydaktyczna/symulacyjna
	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
	Metoda ćwiczeniowa
✓	Metoda laboratoryjna
	Metoda badawcza (dociekania naukowego)
	Metoda warsztatowa
	Metoda projektu
✓	Pokaz i obserwacja
	Demonstracje dźwiękowe i/lub video
	Metody aktywizujące (np.: „burza mózgów”, technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej”, konstruowanie „map myśli”)
✓	Praca w grupach
	Wykład zdalny w czasie rzeczywistym

[illegible]

Projekt		✓								
Esej										
Raport										
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)										
Portfolio										
Zadania cząstkowe na wykładzie										
...										

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		30
Praca własna studenta*	Przygotowanie do zajęć	0
	Czytanie wskazanej literatury	10
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	10
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	5
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	20
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	Inne (jakie?)	
SUMA GODZIN		75
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		3

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 90% punktów
dobry plus (+db; 4,5)	od 80% punktów
dobry (db; 4,0)	od 70% punktów
dostateczny plus (+dst; 3,5)	od 60% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów