	Nazwa modułu **Blok przedmiotów wybieralnych**					Kod modułu: M23	
Wypełnia Zespół Kierunku	Nazwa przedmiotu: **Zarządzanie bezpieczeństwem sieci komputerowych**					Kod przedmiotu:	
	Nazwa jednostki prowadzącej przedmiot / moduł: **INSTYTUT INFORMATYKI STOSOWANEJ**						
	Nazwa kierunku: **INFORMATYKA**						
	Forma studiów: **stacjonarne**		Profil kształcenia: **PRAKTYCZNY**			Specjalność: **Administracja systemów i sieci komputerowych**	
	Rok / semestr: **3/6**		Status przedmiotu /modułu: **obowiązkowy**			Język przedmiotu / modułu: **polski**	
	Forma zajęć	wykład	ćwiczenia	ćwiczenia laboratoryjne	konwersatorium	seminarium	inne (wpisać jakie)
	Wymiar zajęć	**15**		**30**			

Koordynator przedmiotu / modułu	**dr inż. Jerzy Skurczyński**
Prowadzący zajęcia	**Dr inż. Jerzy Skurczyński, mgr Katarzyna Wasielewska**
Cel przedmiotu / modułu	Zapoznanie ze złożonością problemów związanych z bezpieczeństwem w sieciach komputerowych, Nauczenie stosowania mechanizmów zwiększających poziom bezpieczeństwa w sieciach komputerowych, Rozwijanie umiejętności weryfikacji potencjalnych zagrożeń oraz umiejętności opracowywania polityki bezpieczeństwa
Wymagania wstępne	Znajomość podstawowych zagadnień sieciowych związanych z procesami routingu (routing statyczny, RIP, EiGRP, OSPF) i przełączaniem w sieciach IP (STP, VTP, VLAN). Znajomość metod optymalizacji adresowania IP. Podstawy matematyki dyskretnej.

EFEKTY KSZTAŁCENIA		Odniesienie do efektów dla **programu**
Nr	Wiedza	
01	zna rodzaje zagrożeń występujących w sieciach komputerowych	K_W16, K_W17, K_W18
02	zna sposoby zapobiegania zagrożeniom bezpieczeństwa sieci	K_W16, K_W17, K_W18
03	Zna podstawy funkcjonowania sieci teleinformatycznych z uwzględnieniem ich bezpieczeństwa	K_W08
	Umiejętności	
04	Identyfikuje możliwe zagrożenia dla danej sieci komputerowej	K_U10, K_U14
05	Stosuje wybrane środki sprzętowe i programowe zwiększające bezpieczeństwo sieci	K_U10, K_U14
06	Opracowuje politykę bezpieczeństwa	K_U03
07	Realizuje zadania związane z utrzymaniem urządzeń sieciowych w ruchu z uwzględnieniem aspektów bezpieczeństwa	K_U22
	Kompetencje społeczne	
08	skutecznie porozumiewa się z przełożonymi i współpracownikami w celu wspólnego zapewnienia bezpieczeństwa zasobom informacyjnym w sieci komputerowej	K_K04

TREŚCI PROGRAMOWE

Forma zajęć – WYKŁAD

1. Współczesne zagrożenia w sieciach komputerowych
2. Urządzenia sieciowe i ich wpływ na bezpieczeństwo sieci komputerowych
3. Uwierzytelnianie, autoryzacja i kontrola dostępu
4. Firewall
5. Ochrona przed włamaniami do sieci komputerowej
6. Zabezpieczanie sieci LAN przewodowej i bezprzewodowej
7. Szyfrowanie w sieciach komputerowych
8. Sieci VPN

9. Polityka bezpieczeństwa sieci komputerowej
Forma zajęć – LABORATORIUM
Celem laboratorium jest implementacja mechanizmów zwiększających bezpieczeństwo sieci komputerowych: identyfikacja i konfiguracja poziomów uprzywilejowania na urządzeniach sieciowych, konfiguracja uwierzytelniania i autoryzacji, metody dostępu, zaawansowane listy kontroli dostępu, implementacja CBAC i ZBF, mechanizmy bezpieczeństwa routerów i przełączników, sieci VPN, monitoring, polityka bezpieczeństwa sieci, zarządzanie bezpieczną siecią.

Metody kształcenia	1. Wykład z prezentacją multimedialną 2. Ćwiczenia laboratoryjne: planowanie i przeprowadzanie eksperymentów

Metody weryfikacji efektów kształcenia	Nr efektu kształcenia z sylabusa
Egzamin	01, 02, 03
Kolokwium, sprawdzanie bieżących zadań	04, 05
Zadania domowe	06, 07, 08

Forma i warunki zaliczenia	Laboratorium: praca samodzielna; aktywny udział w zajęciach; podstawą zaliczenia jest udział w zajęciach, wykonywanie bieżących zadań praktycznych oraz kolokwium praktyczne podsumowujące zdobytą wiedzę Wykład: zaliczenie pisemne
Literatura podstawowa	1. James F. Kurose, Keith W. Ross, *Sieci komputerowe. Ujęcie całościowe*, Helion 2010 2. M. Szmit, M. Gusta, M. Tomaszewski, *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion 2005 3. W. Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptografii*, Helion 2011 4. M. Stawowski, *Projektowanie i praktyczne implementacje sieci VPN*, ARSKOM 2004
Literatura uzupełniająca	1. M. Serefin, *Sieci VPN. Praca zdalna i bezpieczeństwo danych*, wyd. II rozszerzone, Helion 2009 2. E.D. Zwicky, S. Cooper, D.B. Chapman, *Internet Firewalls - tworzenie zapór ogniowych*, RM, 2001 3. B. Schneier, *Kryptografia dla praktykow*, WNT, 2004

NAKŁAD PRACY STUDENTA:

	Liczba godzin
Udział w wykładach	15
Samodzielne studiowanie tematyki wykładów	10
Udział w ćwiczeniach audytoryjnych i laboratoryjnych*	30
Samodzielne przygotowywanie się do ćwiczeń*	15
Przygotowanie projektu / eseju / itp. *	
Przygotowanie się do egzaminu / zaliczenia	5
Udział w konsultacjach	3
Inne	2
ŁĄCZNY nakład pracy studenta w godz.	80
Liczba punktów ECTS za przedmiot	**3ECTS**
Obciążenie studenta związane z zajęciami praktycznymi*	45 **1,8 ECTS**
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	50 **2 ECTS**