Państwowa Wyższa Szkoła Zawodowa
im. Hipolita Cegielskiego w Gnieźnie

Instytut Elektroniki i Telekomunikacji

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo w sieciach komputerowych	

KARTA OPISU MODUŁU KSZTAŁCENIA

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Elektronika i Telekomunikacja	**praktyczny**	**3/6**
Specjalność	Przedmiot oferowany w języku: **polskim**	Kurs (obligatoryjny/obieralny) **Obieralny**
Godziny: Wykłady: **30** Ćwiczenia: Laboratoria: **15** Projekty / seminaria:		Liczba punktów **4**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)	**Obszar(y) kształcenia**	**Podział ECTS (liczba i %)**
I	**stacjonarne**	**nauki techniczne**	**4** **100%**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) (ogólnouczelniany, z innego kierunku)

specjalnościowy

Jednostka prowadząca przedmiot: **Instytut Elektroniki i Telekomunikacji**

Osoba odpowiedzialna za przedmiot / wykładowca: **Lista osób prowadzących zajęcia:**

dr hab. inż. Mariusz Głąbowski
e-mail: mariusz.glabowski@put.poznan.pl
tel. 61 424 2942
Instytut Elektroniki i Telekomunikacji
ul. Ks. S. Wyszyńskiego 36, 62-200 Gniezno

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Zna pojęcia charakteryzujące sieci telekomunikacyjne i komputerowe oraz rozumie techniczne znaczenie tych pojęć.
2	**Umiejętności:**	brak
3	**Kompetencje społeczne**	Ma świadomość konieczności poszerzania swoich kompetencji oraz gotowość do podjęcia współpracy w ramach zespołu

Cel przedmiotu:

Poznanie teoretycznych i praktycznych zagadnień związanych z budowaniem bezpiecznych sieci komputerowych (teleinformatycznych) oraz z świadomym i bezpiecznym korzystaniem z zasobów Internetu.

Efekty kształcenia

Wiedza. W wyniku przeprowadzonych zajęć student powinien/ będzie w stanie:		Odniesienie do Kierunkowych Efektów Kształcenia
01	Student posiada wiedzę z zakresu protokołów wykorzystywanych do zapewnienia bezpieczeństwa sieci komputerowych	**K1_W19++**
02	Ma praktyczną wiedzę na temat systemów bezpieczeństwa i metod umożliwiających zapewnienie bezpieczeństwa informacji przesyłanych w sieciach komputerowych i telekomunikacyjnych. Rozumie na czym polegają zasady prawidłowej konstrukcji polityk bezpieczeństwa dla sieci teleinformatycznych.	**K1_W22+++**
Umiejętności. W wyniku przeprowadzonych zajęć student będzie potrafił:		Odniesienie do Kierunkowych Efektów Kształcenia

03	Potrafi wykorzystywać technologie umożliwiające bezpieczne przesyłanie danych w sieciach rozległych. Potrafi skonfigurować urządzenia sieciowe z uwzględnieniem polityk bezpieczeństwa	**K1_U23+++**
04	Potrafi przygotować opracowanie dotyczące wdrożenia polityk bezpieczeństwa w urządzeniach sieciowych.	**K1_U03+**
Kompetencje społeczne. W wyniku przeprowadzonych zajęć student zdobędzie następujące kompetencje:		Odniesienie do Kierunkowych Efektów Kształcenia
01	Dąży do ciągłej aktualizacji wiedzy i umiejętności z zakresu bezpieczeństwa sieci	**K1_K01**
01	Profesjonalnie podchodzi do rozwiązywania problemów związanych z bezpieczeństwem sieci	**K1_K02**
03	Ma poczucie odpowiedzialności za zaprojektowane systemy bezpieczeństwa sieci	**K1_K03**
04	Posiada świadomość wpływu zagrożeń bezpieczeństwa sieci telekomunikacyjnych i teleinformatycznych na kształtowanie społeczeństwa informacyjnego.	**K1_K04**

Sposoby sprawdzenia efektów kształcenia

Wykład

- pisemny egzamin – sprawdzenie wiedzy

Laboratoria:

- sprawdzian i premiowanie przyrostu wiedzy niezbędnej do realizacji postawionych problemów w danym obszarze tematyki przedmiotu;
- ocenianie ciągłe, na każdych zajęciach - premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami;
- ocena poprawności działania w ramach pracy własnej.

Treści programowe

W trakcie wykładów poruszane będą następujące zagadnienia:

1. Analiza zagrożeń płynących Internetu
2. Sprzętowe i programowe zapory sieciowe (firawalls)
3. Bezpieczeństwo urządzeń sieciowych
4. Systemy wykrywania włamań (IDS/IPS)
5. Podstawy kryptografii
6. Protokoły sieciowe zapewniające bezpieczne przesyłanie danych
7. Wirtualne Sieci Prywatne - VPN (Virtual Private Network)
8. Testy bezpieczeństwa systemów informatycznych

Literatura podstawowa:

1. Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Marek Serafin, Helion 2009/12
2. Bezpieczeństwo sieci, E. Cole, R. Krutz, J. Conley, Helion, 2005
3. 101 zabezpieczeń przed atakami w sieci komputerowej, Maciej Szmit, Marek Gusta, Mariusz Tomaszewski, Helion 2005

Literatura uzupełniająca:

CCNA Security Official Exam Certification Guide, Michael Watkins, Kevin Wallace - Cisco Press (2008)

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo w sieciach komputerowych	

Obciążenie pracą studenta		
forma aktywności	**godzin**	**ECTS**
Łączny nakład pracy	125[1)]	4
Zajęcia wymagające indywidualnego kontaktu z nauczycielem	53[2)]	3
Zajęcia o charakterze praktycznym	80[3)]	3

1 pkt ECTS≈ 25-30 h pracy studenta – do określenia poszczególnych składowych proszę przyjąć dotychczasową liczbę punktów.

1) – łączne obciążenie studenta

2) - zajęcia dydaktyczne {w+c+L+p} + konsultacje +egzamin; dla stacjonarnych liczba godzin > 50 % godzin z poz1.

3) Zajęcia laboratoryjne+przygotowanie do tych zajęć+opracowanie sprawozdań+zajęcia projektowe+przygotowanie do zajęć projektowych+konsulatcje w sprawie projektów+realizacja projektu.

UWAGA: Zaleca się opis efektów kształcenia dla przedmiotu (modułu) od 4 – 8 pozycji.