KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo w sieciach komputerowych	**1010822121010821006**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Elektronika i Telekomunikacja	**ogólnoakademicki**	**1 / 2**
Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Sieci komputerowe i technologie	**polski**	**obieralny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
II stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **2** Ćwiczenia: **1** Laboratoria: **1** Projekty/seminaria: **-**	**4**

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

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**4 100%**
nauki techniczne	**4 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Sławomir Hanczewski
email: slawomir.hanczewski@et.put.poznan.pl
tel. +48 61 665 39 46
Wydział Elektroniki i Telekomunikacji
ul. Piotrowo 3A 60-965 Poznań

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Sławomir Hanczewski
email: slawomir.hanczewski@et.put.poznan.pl
tel. +48 61 665 39 46
Wydział Elektroniki i Telekomunikacji
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	K1_W22 (część) Zna pojęcia charakteryzujące sieci telekomunikacyjne i komputerowe oraz rozumie techniczne znaczenie tych pojęć. Ma uporządkowaną podstawową wiedzę w zakresie struktury, funkcjonowania i standardów różnego typu sieci komputerowych i telekomunikacyjnych. Zna podstawy inżynierii ruchu, teorii kolejek, usług, urządzeń, systemów zarządzania, protokołów sieciowych i technik telekomunikacyjnych, które są wykorzystywane w sieciach telekomunikacyjnych i komputerowych.
2	**Umiejętności:**	K1_U25 Potrafi skonfigurować urządzenia i uruchomić lokalną sieć komputerową. Potrafi dokonać wyboru właściwego algorytmu dla potrzeb rozwiązywanego sieciowego problemu optymalizacyjnego. Potrafi wykorzystywać aplikacje analizujące ruch w sieciach LAN oraz aplikacje umożliwiające bezpieczne przesyłanie danych.
3	**Kompetencje społeczne**	K1_K03 Ma poczucie odpowiedzialności za zaprojektowane systemy elektroniczne i telekomunikacyjne i zdaje sobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego wykorzystania

Cel przedmiotu:

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

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Student posiada wiedzę z zakresu bezpieczeństwa sieci komputerowych. - [K2_W12]

Umiejętności:

1. Potrafi konfigurować urządzenia sieciowe i oprogramowanie w sposób zapewniający bezpieczene przesyłanie danych. Potrafi świadomie korzystać z zasobów Internetu - [K2_U14]

Kompetencje społeczne:

1. Dąży do ciągłej aktualizacji wiedzy i umiejętności z zakresu bezpieczeństwa sieci - [K2_K04]
2. Profesjonalnie podchodzi do rozwiązywania problemów związanych z bezpieczeństwem sieci - [K2_K05]

Sposoby sprawdzenia efektów kształcenia

Wykład - egzamin ustny

Laboratorium - sprawdzenie przygotowania studentów do zajęć(sprawdzian wejściowy), praktyczne sprawdzenie umiejętności studentów z zakresu bezpieczeństwa,

Ćwiczenia - sprawdzian

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:

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

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Udział w wykładach, laboratoriach i ćwiczeniach	60
2. Przygotowanie do laboratoriów i ćwiczeń	20
3. Przygotowania sprawozdań	10
4. Przygotowanie do egzaminu	10
5. Egzamin	2
6. Konsultacje	3

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	105	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	65	2
Zajęcia o charakterze praktycznym	50	2