

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Security in Communication Networks</b>		Kod <b>1010802121010822890</b>
Kierunek studiów <b>Electronics and Telecommunications</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>ogólnoakademicki</b>	Rok / Semestr <b>1 / 2</b>
Ścieżka obieralności/specjalność <b>Information and Communication</b>	Przedmiot oferowany w języku: <b>Polish / English</b>	Kurs (obligatoryjny/obieralny) <b>obieralny</b>
Stopień studiów: <b>II stopień</b>	Forma studiów (stacjonarna/niestacjonarna) <b>stacjonarna</b>	
Godziny Wykłady: <b>2</b> Ćwiczenia: -   Laboratoria: <b>2</b> Projekty/seminaria: -	Liczba punktów <b>5</b>	
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) <b>kierunkowy</b>		(ogólnouczelniany, z innego kierunku) <b>z danego kierunku</b>
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki <b>nauki techniczne</b>  <b>nauki techniczne</b>		Podział ECTS (liczba i %) <b>100 5%</b>  <b>100 5%</b>
<b>Odpowiedzialny za przedmiot / wykładowca:    Odpowiedzialny za przedmiot / wykładowca:</b>		
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		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
<b>Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:</b>		
1	<b>Wiedza:</b>	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	<b>Umiejętności:</b>	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	<b>Kompetencje społeczne</b>	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
<b>Cel przedmiotu:</b> Poznanie teoretycznych i praktycznych zagadnień związanych z budowaniem bezpiecznych sieci komputerowych (teleinformatycznych) oraz z świadomym i bezpiecznym korzystaniem z zasobów Internetu.		
<b>Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia</b>		
<b>Wiedza:</b> 1. Student posiada wiedzę z zakresu bezpieczeństwa sieci komputerowych. - [K2_W12]		
<b>Umiejętności:</b> 1. Potrafi konfigurować urządzenia sieciowe i oprogramowanie w sposób zapewniający bezpieczne przesyłanie danych. Potrafi świadomie korzystać z zasobów Internetu - [K2_U14]		
<b>Kompetencje społeczne:</b> 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]		
<b>Sposoby sprawdzenia efektów kształcenia</b>		

<p>Wykład - egzamin ustny          Laboratorium - sprawdzenie przygotowania studentów do zajęć(sprawdzian wejściowy), praktyczne sprawdzenie umiejętności studentów z zakresu bezpieczeństwa,          Ćwiczenia - sprawdzian</p>		
<b>Treści programowe</b>		
<p>W trakcie wykładów poruszane będą następujące zagadnienia:</p> <ol style="list-style-type: none"> <li>1. Analiza zagrożeń płynących Internetu</li> <li>2. Sprzętowe i programowe zapory sieciowe (firawalls)</li> <li>3. Bezpieczeństwo urządzeń sieciowych</li> <li>4. Systemy wykrywania włamań (IDS/IPS)</li> <li>5. Podstawy kryptografii</li> <li>6. Protokoły sieciowe zapewniające bezpieczne przesyłanie danych</li> <li>7. Wirtualne Sieci Prywatne - VPN (Virtual Private Network)</li> <li>8. Testy bezpieczeństwa systemów informatycznych</li> </ol>		
<b>Literatura podstawowa:</b>		
<ol style="list-style-type: none"> <li>1. A Guide to Computer Network Security, Joseph Migga Kizza, Springer 2009</li> <li>2. Network Security: Private Communication in a Public World (2nd Edition) Charlie Kaufman, Radia Perlman, Mike Speciner</li> <li>3. Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide) Catherine Paquet , Ciscopress.com, 2009</li> <li>4. CCNA Security Official Exam Certification Guide, Michael Watkins, Kevin Wallace - Cisco Press 2008</li> </ol>		
<b>Literatura uzupełniająca:</b>		
<ol style="list-style-type: none"> <li>1. A Guide to Computer Network Security, Joseph Migga Kizza, Springer 2009</li> </ol>		
<b>Bilans nakładu pracy przeciętnego studenta</b>		
<b>Czynność</b>		<b>Czas (godz.)</b>
1. Udział w wykładach, laboratoriach i ćwiczeniach		60
2. Przygotowanie do laboratoriów i ćwiczeń		20
3. Przygotowania sprawozdań		20
4. Przygotowanie do egzaminu		20
5. Egzamin		2
6. Konsultacje		3
<b>Obciążenie pracą studenta</b>		
<b>forma aktywności</b>	<b>godzin</b>	<b>ECTS</b>
Łączny nakład pracy	125	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	65	2
Zajęcia o charakterze praktycznym	50	2