POLITECHNIKA RZESZOWSKA im. I. Łukasiewicza

WYDZIAŁ	Wydział Elektrotechniki i Informatyki
KIERUNEK	Informatyka (EF)
SPECJALNOŚĆ	FDA
FORMA I STOPIEŃ STUDIÓW	DI - stacjonarne I stopnia

KARTA PRZEDMIOTU

NAZWA PRZEDMIOTU	**Bezpieczeństwo systemów informatycznych**

Nauczyciel odpowiedzialny za przedmiot: dr inż. Marcin Bednarek

Kontakt dla studentów: tel. 0178651543 **e-mail: bednarek@prz.rzeszow.pl**

Nauczyciel/e prowadzący: dr inż. Marcin Bednarek

Katedra/Zakład/Studium Katedra Informatyki i Automatyki

Semestr	całkowita liczba godzin	W	C	L	P (S)	ECTS
6	45	25		20		3

PRZEDMIOTY POPRZEDZAJĄCE WRAZ Z WYMAGANIAMI
Sieci komputerowe (protokoły komunikacyjne)

TREŚCI KSZTAŁCENIA WG PROWADZONYCH RODZAJÓW ZAJĘĆ	LICZBA GODZIN
Wykład: Bezpieczeństwo informacyjne. Polityka bezpieczeństwa. Zagrożenia bezpieczeństwa. Ataki na bezpieczeństwo. Usługi bezpieczeństwa, mechanizmy zabezpieczające. Certyfikacja systemów. Podstawy kryptografii. Rodzaje szyfrów. Szyfrowanie klasyczne. Systemy szyfrowania symetryczne blokowe i strumieniowe. Szyfrowanie z użyciem klucza publicznego. PGP. Algorytmy kryptograficzne symetryczne i asymetryczne. Metody uwierzytelniania. Podpis elektroniczny. Watermarking i steganografia. Programy złośliwe. Emisja ujawniająca. Zapory sieciowe. Sniffing i scanning. Kopie bezpieczeństwa. Ochrona informacji w sieciach teleinformatycznych (m.in. sieci komputerowe, bezprzewodowe sieci komputerowe, przesył satelitarny). Sieci wirtualne (tunelowanie). Zabezpieczenia transmisji w komputerowych sieciach przemysłowych i rozproszonych systemach sterowania.	25
Ćwiczenia:	

Laboratorium: Analizowanie i/lub projektowanie bezpieczeństwa systemów informatycznych, sieci komputerowych. Implementacja usług i mechanizmów bezpieczeństwa w systemach informatycznych. Bezpieczeństwo sieci komputerowych. Wirtualne sieci prywatne. Zapory ogniowe. Scanning i sniffing. Prawa dysponenckie eDirectory i/lub Active Directory. Bezpieczeństwo przechowywania danych.	20
Dyżury dydaktyczne (konsultacje): w terminach podanych w harmonogramie pracy jednostki	
EFEKTY KSZTAŁCENIA - UMIEJĘTNOŚCI KSZTAŁCENIA	
Umiejętność analizowania i projektowania bezpieczeństwa systemów informatycznych.	

FORMA I WARUNKI ZALICZENIA PRZEDMIOTU (RODZAJU ZAJĘĆ)
Wykład: pozytywna ocena z pisemnego testu, zaliczenie ustne. Laboratorium: pozytywna ocena wykonanych zadań laboratoryjnych (dokumentacja) i z pisemnego testu.

WYKAZ LITERATURY PODSTAWOWEJ
1. Stamp M.: Information Security. Principles and Practice. Willey-Interscience, Hoboken, 2006. 2. Stallings W.: Ochrona danych w sieci i intersieci. W teorii i praktyce. WNT, Warszawa 1997 3. Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa – Poznań 2001 4. Liderman K.: Bezpieczeństwo Teleinformatyczne, Instytut Automatyki i Robotyki WAT, Warszawa 2001 5. Anderson J.: Security Engineering. A Guide to Building Dependable Distributed Systems, Wiley Publishing Inc., Indianapolis 2008 6. Maiwald E. Bezpieczeństwo w sieci: kurs podstawowy, EDITION 2000, Kraków 2001 7. Sutton R. J.: Bezpieczeństwo telekomunikacji: praktyka i zarządzanie, WKiŁ, Warszawa 2004 8. Smith B., Komar B, Microsoft Security Team: Windows Security, APN Promise, Warszawa 2003

WYKAZ LITERATURY UZUPEŁNIAJĄCEJ
1. Schneier B.: Kryptografia dla praktyków, WNT, Warszawa 2002 2. Dennig D.E.: Wojna informacyjna i bezpieczeństwo informacji, WNT, Warszawa 2002 3. Put D.: Szkoła Hakerów - podręcznik, Wydawnictwo CHS, Kwidzyn 2006

Podpis nauczyciela odpowiedzialnego za przedmiot	
Podpis kierownika katedry (zakładu/studium)	
Data i podpis dziekana właściwego wydziału	