POLITECHNIKA RZESZOWSKA im. I. Łukasiewicza

WYDZIAŁ	Wydział Elektrotechniki i Informatyki
KIERUNEK	Telekomunikacja
SPECJALNOŚĆ	
FORMA I STOPIEŃ STUDIÓW	Studia stacjonarne I-go stopnia

KARTA PRZEDMIOTU

NAZWA PRZEDMIOTU	**Kryptografia i bezpieczeństwo danych**

Nauczyciel odpowiedzialny za przedmiot: **dr inż. Kazimierz Lal**

Kontakt dla studentów: tel. 48178651767 **e-mail: klal@prz-rzeszow.pl**

Nauczyciel/e prowadzący: dr inż. Kazimierz Lal, dr inż. Tomasz Rak

Katedra/Zakład/Studium Katedra Informatyki i Automatyki

Semestr	całkowita liczba godzin	W	C	L	P (S)	ECTS
6	45	30		15		3

PRZEDMIOTY POPRZEDZAJĄCE WRAZ Z WYMAGANIAMI

TREŚCI KSZTAŁCENIA WG PROWADZONYCH RODZAJÓW ZAJĘĆ	LICZBA GODZIN
Wykład: Wprowadzenie do bezpieczeństwa systemów informatycznych – świadomość użytkownika, podstawy kryptografii, typy szyfrów, tryby szyfrowania. Współczesne algorytmy kryptograficzne - symetryczne algorytmy szyfrujące, algorytmy z kluczem publicznym, podpis cyfrowy, kody uwierzytelniania wiadomości. Infrastruktura klucza publicznego - norma X.509, organizacja i zarządzanie CA, elementy składowe infrastruktury PKI. Uwierzytelnianie i autoryzacja – metody uwierzytelniania i autoryzacji obiektów w systemach operacyjnych Linux, Unix oraz Windows. Bezpieczeństwo przechowywania danych – szyfrowanie plików, generowanie podpisu cyfrowego, macierze dyskowe RAID, urządzenia i oprogramowanie do zabezpieczania danych, układy zasilania rezerwowego, zarządzanie nośnikami z danymi wrażliwymi. Bezpieczeństwo transmisji w danych – protokoły PGP, S/MIME, SSL/TLS, SSH, IPSec.	28+2 zaliczenie

Typy "ścian ogniowych" (Firewalls). Zastosowanie OpenSSL do szyfrowania plików, generowania kluczy, podpisu cyfrowego, tworzenia centrum certyfikacji CA, generacji certyfikatów dla serwerów WWW. Wykorzystanie SSH do bezpiecznej komunikacji z komputerem zdalnym.	
Ćwiczenia:	
Laboratorium: Instalacja centrum autoryzacji w Windows serwer 2008. Instalacja usług katalogowych e-Directory na serwerze SLES10. Instalacja i konfiguracja połączeń IPSec na bazie wybranego systemu operacyjnego. Instalacja, konfiguracja i testowanie macierzy dyskowych – sprzętowych i programowych. Konfiguracja i testowanie Firewall-a. Instalacja i testowanie wybranych narzędzi do szyfrowania danych w stacjach roboczych. Narzędzia do testowania bezpieczeństwa sieci komputerowych. **Projekt:**	3 2 2 2 2 2 2
Dyżury dydaktyczne (konsultacje): w terminach podanych w harmonogramie pracy jednostki;	
EFEKTY KSZTAŁCENIA - UMIEJĘTNOŚCI I KWALIFIKACJE	
Student powinien pozyskać teoretyczną wiedzę i praktyczne zrozumienie tematu przedmiotu. Zdobywa umiejętność zabezpieczania sieci komputerowych.	

FORMA I WARUNKI ZALICZENIA PRZEDMIOTU (RODZAJU ZAJĘĆ)
Egzamin końcowy, pisemne lub ustne sprawdzenie wiedzy na każdym laboratorium, test z laboratorium.

WYKAZ LITERATURY PODSTAWOWEJ
Kutyłowski M., Strothmann W.: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych. Oficyna Wydawnicza Read Me. Warszawa, 1999; Mochnacki W.: Kody korekcyjne i kryptografia. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław, 2000; Stallings W.: Ochrona danych w sieci i intersieci – w teorii i praktyce. WNT, Warszawa, 1997; Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych. PWN, Warszawa, 2001; Welschenbach M.: Kryptografia w C i C++, Mikom, Warszawa, 2002.

WYKAZ LITERATURY UZUPEŁNIAJĄCEJ
Sportack M.: Sieci komputerowe Księga eksperta, Wydanie II – poprawione, HELION, 2004; Hunt C.: TCP/IP - Administracja sieci, RM, 2003 ; Lal K., Rak T.: Linux a technologie klastrowe, PWN-MIKOM, 2005;

Lal K., Rak T.: Po prostu własny serwer internetowy, HELION, 2002; Rak T.: Tworzenie sieci komputerowej. Ćwiczenia praktyczne, HELION, 2006.

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