**Nazwa przedmiotu:**

Bezpieczeństwo systemów informatycznych

**Koordynator przedmiotu:**

dr inż. Bartosz Sawicki, bartosz.sawicki@ee.pw.edu.pl, +48222345760
sawickib@iem.pw.edu.pl
tel: 5760

**Status przedmiotu:**

Fakultatywny ograniczonego wyboru

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Elektrotechnika

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

2 / rok ak. 2011/2012

**Liczba punktów ECTS:**

2

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 15h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Budowa i konfiguracja systemów operacyjnych. Działanie sieci komputerowych. Podstawy programowania, Podstawy matematyki

**Limit liczby studentów:**

**Cel przedmiotu:**

Umiejętność dostrzegania aspektów bezpieczeństwa w podczas działania systemów informatycznych.Przedmiot obejmuje szerokie spektrum zagadnień, których celem jest uświadomienie studentowi potencjalnych zagrożeń, prewencji i metod obrony przed celowymi atakami, a także przypadkowymi awariami. Prezentowana wiedza rozszerzy umiejętności zarówno programisty, administratora systemu oraz menadzera IT.

**Treści kształcenia:**

Szczegółowe treści programowe przedmiotu, poszczególnych zajęć, Należy uwzględnić treści merytoryczne przedmiotu dla każdej składowej przedmiotu tj. dla W; Ć; L; P.

W1. Wprowadzenie do kryptologii. Kryptografia i kryptoanaliza historyczna.
L1. Ćwiczenia z krytografią historyczną w programie CrypTool.
W2. Współczesna kryptografia. Problemy prawne. Zasady Kerckhoffa. Teoria Shanona. Szyfrowanie XOR, OTP.
W3. Szyfry blokowe DES, AES, IDEA. Tryby pracy szyfrów blokowych: ECB, CBC, CFB. Szyfry strumieniowe: RC4.
W4. Idea szyfrowania asymetrycznego. Szyfry asymetryczne: RSA, ElGamal, ECC.
L2. Ćwiczenia z kryptografii współczesnej programie CrypTool.
W5. Funkcje skrótu i ich zastosowania. Algorytm MD5, SHA. Ataki na funkcje skrótu. Ćwiczenia w programie CrypTool.
L3 Konfiguracja bezpiecznych serwisów sieciowych (Apache). Zabezpieczanie zasobów na hasło.
L4 Konfiguracja bezpiecznych serwisów sieciowych (Apache+SSL). Generowanie i podpisywanie certyfikatów.
W6 Bezpieczeństwo ruchu w sieciach komputerowych. Podsłuch, analizatory ruchu, wykrywanie ataków.
L5 Programy( tcpdump, nmap, snort, nessus).
W7 Metody i prokoły uwierzytelniania
L6 Ataki na protokoły uwierzytelniania (ćwiczenia w Cryptoolu).
W8 Tworzenie bezpiecznych programów. Zalecenia ogólne, błąd przepełnienia bufora.
L7 Demonstracja w Javie, i ćwiczenia w języku C.
W9 Bezpieczne programowanie webowe. Javascript. AJAX. Ataki SQLInjection, XSS.
L8 Zabawu typu Hack-Me: http://quiz.ngsec.com/, http://uw-team.org
W10 Bezpieczne programowanie webowe - kontynuacja.
W11 Polityka bezpieczeństwa obiegu informacji w firmie. Dokument polityki bezpieczeństwa. Norma PN-ISO/IEC 17799.
L 9. Ćwiczenie z tworzenia dokumentu polityki bezpieczeństwa dla przykładowej firmy. Optymalizacja poziomu zabezpieczeń.
W12 Kluczowe elementy praktycznej ochrony danych. Podstawy audytu bezpieczeństwa.

**Metody oceny:**

**Egzamin:**

**Literatura:**

“Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych”. Kutyłowski Mirosław, Strothmann Willy-B; Wydawnictwo Read Me, 2000
“Kryptografia. W teorii i w praktyce” Douglas R. Stinson; WNT, Warszawa, 2005

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe