**Nazwa przedmiotu:**

Ochrona danych w systemach informatycznych

**Koordynator przedmiotu:**

dr inż. Bartosz Sawicki, bartosz.sawicki@ee.pw.edu.pl, +48222345760

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

4 / rok ak. 2011/2012

**Liczba punktów ECTS:**

4

**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:  | 30h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Podstawy informatyki, Podstawy teorii mnogości i mat. dyskretnej, Systemy operacyjne, Sieci komputerowe

**Limit liczby studentów:**

**Cel przedmiotu:**

Teoretyczne podstawy bezpieczeństwa systemów informatycznych. Algorytmy kryptograficzne i ich zastosowania.. Tworzenie bezpiecznych aplikacji komputerowych. Konfigurowanie bezpiecznych serwerów i usług sieciowych. Zarządzanie bezpieczeństwem na przykładzie dokumentu polityki bezpieczeństwa i audytu bezpieczeństwa.

**Treści kształcenia:**

Wykład
1. Wprowadzenie. Kryptografia, steganografia. Definicje pojęć. Rys historyczny. Algorytmy historyczne.
2. Współczesna kryptografia. Problemy prawne. Szyfrowanie XOR, OTP, DES.
3. Szyfry blokowe: IDEA, RC5, AES. Tryby pracy szyfrów blokowych: ECB, CBC, CFB.
4. Generowanie liczb losowych. Szyfry strumieniowe: RC4. Idea szyfrowania asymetrycznego. Arytmetyka modularna. Szyfr plecakowy.
5. Szyfrowanie asymetryczne: RSA, ElGamal, ECC.
6. Funkcje jednokierunkowe. Funkcje skrótu i ich zastosowania. Ataki na funkcje skrótu. Algorytm MD5.
7. Podpis cyfrowy. Możliwości i ograniczenia. DSA. Ślepy podpis przy pomocy RSA. Podpisy niezaprzeczalne.
8. Uwierzytelnianie, a autoryzacja. Tajne hasło, 'wyzwanie-odpowiedź', dowody iteracyjne, dowody z wiedzą zerową. Protokół Fiata-Shamira.
9. Protokoły uzgadniania kluczy. Atak 'man-in-the-middle'. Protokół Diffie-Hellmana. Protokół interlock.
10. Protokóły dzielenia tajemnic. Protokóły zobowiązania bitowego.
11. Realne problemy bezpieczeństwa danych. Omówienie popularnych programów: Kerberos, SSH, SSL/TLS
12. Modele bezpieczeństwa. Polityki kontroli dostępu: uznaniowa, obowiązkowa. Model macierzowy. Model
'przejmij-przekaż'.
13. Bezpieczne programowanie. Projektowanie aplikacji, błędy programistyczne (przepełnienie bufora),
walidacja danych, aplikacje internetowe.
14. Polityka bezpieczeństwa. Zarządzanie ryzykiem. Norma PN-ISO/IEC 17999. Zasady i rodzaje audytu
bezpieczeństwa.
Laboratorium
1. Zajęcia organizacyjne. Wykład przypominający podstawy pracy w trybie linii poleceń. Krótkie wprowadzenie do programowania w Shellu i Perlu.
2. Algorytmy kryptografii w zastosowaniach programistycznych (Perl).
3. Algorytmy kryptoanalizy w zastosowaniach programistycznych (Perl).
4. Zastosowanie wybranych programów służących do ochrony danych (GPG, SSH).
5. Bezpieczne programowanie, błąd przepełnienia bufora i inne.
6. Wprowadzenie do technologii serwerów wirtualnych.
7. Instalacja systemu FreeBSD.
8. Zarządzanie oprogramowaniem w systemie FreeBSD.
9. Konfiguracja bezpiecznych serwisów sieciowych (Apache+SSL).
10. Analiza ruchu i zagrożeń sieciowych.
11. Serwery sieciowe, usługi katalogowe, udostępnianie zasobów dyskowych.
12. Zabezpieczenie kompletnego systemu.
13. Zabezpieczenie kompletnego systemu c.d.
14. Audyt bezpieczeństwa systemu.
15. Zakończenie zajęć. Wpisy.

**Metody oceny:**

brak

**Egzamin:**

**Literatura:**

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

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe