

Tytuł <b>Bezpieczeństwo informacji w Internecie</b>	Kod <b>1010332421010330684</b>
Kierunek <b>Informatyka</b>	Rok / Semestr <b>1 / 2</b>
Specjalność -	Przedmiot <b>obowiązkowy</b>
Godziny Wykłady: <b>2</b> Ćwiczenia: -    Laboratoria: <b>1</b> Projekty / seminaaria: -	Liczba punktów <b>6</b>
	Język prowadzenia przedmiotu <b>polski</b>

**Prowadzący:**

dr hab. inż. Janusz Stokłosa, prof. nadzw.  
Instytut Automatyki i Inżynierii Informatycznej  
tel. +48 61 665 37 57  
e-mail: janusz.stoklosa@put.poznan.pl

**Wydział:**

Wydział Elektryczny  
ul. Piotrowo 3A  
60-965 Poznań  
tel. (061) 665-2539, fax. (061) 665-2548  
e-mail: office\_deef@put.poznan.pl

**Miejsce przedmiotu w programie studiów:**

Information Security on Internet

**Założenia i cele przedmiotu:**

Celem przedmiotu jest zapoznanie studentów z wybranymi protokołami kryptograficznymi stosowanymi w Internecie.

**Treści programowe przedmiotu (opis przedmiotu):**

Wykłady obejmują:

1. Standaryzacja - ISO/IEC, IETF, IANA
  2. TLS
  3. IPsec (ESP, AH, ISAKMP, IKE)
  4. PKIX (Profile, protokoły LDAP i OSCP, weryfikacja on-line statusu certyfikatu, polityka certyfikacji)
  5. PKCS (Biblioteki kryptograficzne, PKCS #11 - Cryptoki)
  6. Znakowanie czasem
  7. Radiowy dostęp do Internetu (GSM, UMTS) - algorytmy kryptograficzne
- Ćwiczenia laboratoryjne ilustrują treści przekazywane na wykładzie.

**Przedmioty wprowadzające i wymagane wiadomości wstępne:**

Podstawy ochrony danych, Sieci komputerowe.

**Forma zajęć i metody dydaktyczne:**

Wykład ilustrowany slajdami, ćwiczenia laboratoryjne przy komputerze

**Forma i warunki zaliczenia przedmiotu – wymagania i system oceniania:**

Egzamin pisemny lub ustny lub pisemny i ustny, zaliczenie ćwiczeń laboratoryjnych.

**Bibliografia podstawowa:**

-

**Bibliografia uzupełniająca:**

-