

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Bezpieczeństwo informacji w Internecie		Kod 1010332421010334336
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) (brak)	Rok / Semestr 1 / 2
Ścieżka obieralności/specjalność Technologie informatyczne	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: II stopień	Forma studiów (stacjonarna/niestacjonarna) stacjonarna	
Godziny Wykłady: 2 Ćwiczenia: - Laboratoria: 1 Projekty/seminaria: -		Liczba punktów 5
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) (brak)		(ogólnouczelniany, z innego kierunku) (brak)
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki nauki techniczne		Podział ECTS (liczba i %) 5 100%

Odpowiedzialny za przedmiot / wykładowca:

dr hab. inż. Janusz Stokłosa, prof. nadzw.
email: janusz.stoklosa@put.poznan.pl
tel. +48 61 665 37 57
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	Wiedza:	Ma pogłębioną wiedzę w zakresie bezpieczeństwa danych. Ma pogłębioną wiedzę w zakresie kryptografii i wstępna w zakresie kryptoanalizy.
2	Umiejętności:	Potrafi stosować zaawansowane narzędzia i technologie informatyczne.
3	Kompetencje społeczne	Rozumie potrzebę przekazywania społeczeństwu informacji dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać informacje w sposób zrozumiały, przedstawiając różne punkty widzenia.

Cel przedmiotu:

Celem przedmiotu jest zapoznanie studentów z wybranymi protokołami kryptograficznymi stosowanymi w Internecie, zasadami ich projektowania i użytkowania.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

- Ma wiedzę o aktualnych trendach dotyczących zastosowań informatyki oraz kluczowych problemów z tym związanych. - [K_W06]
- Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zakresie informatyki - [K_W14]

Umiejętności:

- Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie. - [K_U01]
- Potrafi zaproponować i uzasadnić ulepszenia istniejących rozwiązań informatycznych. - [K_U12]

Kompetencje społeczne:

- Potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy. - [K_K01]

Sposoby sprawdzenia efektów kształcenia

Wykład zaliczany jest na podstawie egzaminu pisemnego; kontynuacją egzaminu pisemnego może być egzamin ustny. Kryterium formalnym zdania egzaminu pisemnego jest uzyskanie więcej niż połowę maksymalnej liczby punktów zsumowanych za wszystkie uzyskane odpowiedzi.

Ćwiczenia laboratoryjne zaliczane są na podstawie testu.

Treści programowe

Wykłady obejmują następujące zagadnienia: standaryzacja, TLS, IPsec (ESP, AH, ISAKMP, IKE), PKIX (Profile, protokoły LDAP i OSCP, weryfikacja on-line statusu certyfikatu, polityka certyfikacji), PKCS (Biblioteki kryptograficzne, PKCS #11 - Cryptoki), znakowanie czasem, radiowy dostęp do Internetu - algorytmy kryptograficzne, sieci anonimowe.
 Laboratoria obejmują następujące zagadnienia: protokoły SSL, TLS, S-http, certyfikaty cyfrowe, publiczny system kryptograficzny ? implementacja w oparciu o RSA, bezpieczeństwo komunikacji - Secure Shell, algorytmy kryptograficzne radiowego dostępu do Internetu.

Literatura podstawowa:

1. Bezpieczeństwo danych w systemach informatycznych., J. Stokłosa, T. Bilski, T. Pankowski, Wydawnictwo Naukowe PWN, 2001.
2. Ochrona danych w sieci i intersieci., W. Stallings, WNT, Warszawa, 1997.
3. RFC., <http://www.ietf.org/rfc.html>

Literatura uzupełniająca:

1. Digital Signature Schemes., B. Pfitzmann, Springer, Berlin, 1996.
2. Protection and Security on the Information Superhighway, F. B. Cohen, J. Wiley, New York, 1995.
3. Wybrane artykuły z Lecture Notes in Computer Science, Springer

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Wykłady	30
2. Laboratoria	15
3. Beżące przygotowanie do laboratorium	15
4. Wykonanie sprawozdań z laboratorium	10
5. Przygotowanie do sprawdzianu	10
6. Przygotowanie do egzaminu	35
7. Udział w konsultacjach i egzaminie	10

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	125	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2
Zajęcia o charakterze praktycznym	25	1