KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Podstawy ochrony danych	**1010331551010334967**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**(brak)**	**3 / 5**
Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
-	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
I stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **30** Projekty/seminaria: **-**	**6**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
(brak)	**(brak)**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Anna Grocholewska-Czuryło
email: anna.grocholewska-czurylo@put.poznan.pl
tel. 61-665 35 31
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie podstawowych algorytmów i ich analizy, technik projektowania algorytmów, abstrakcyjnych struktur danych i ich implementacji, problemów obliczeniowo trudnych. Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie technologii sieciowych.
2	**Umiejętności:**	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.
3	**Kompetencje społeczne**	Potrafi konstruować algorytmy z wykorzystaniem podstawowych technik algorytmicznych i dokonać analizy ich złożoności.

Cel przedmiotu:

Celem przedmiotu jest zapoznanie studentów z metodami ochrony danych w systemach informatycznych i wyrobienie umiejętności ich stosowania w praktyce.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie ochrony danych i bezpieczeństwa systemów informatycznych - [K_W13]

Umiejętności:

1. Potrafi zastosować odpowiednie metody ochrony danych i zapewnić bezpieczeństwo systemu informatycznego - [K_U17]

Kompetencje społeczne:

1. Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i poszanowania różnorodności poglądów i kultur. - [K_K03]

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 zalicza się na podstawie obecności, wykonanych ćwiczeń, jakości sprawozdań i sprawdzianu końcowego.

Treści programowe

Na wykładach przekazywane są następujące zagadnienia: Bezpieczeństwo, przestępstwa, środki ochrony. Polityka bezpieczeństwa (ochrona fizyczna, techniczna, prawna, administracyjna). Ochrona antywirusowa. Zasilacze awaryjne. Składowanie danych. Śluzy bezpieczeństwa. Systemy wykrywania włamań. Systemy prewencyjne. Dziennik zdarzeń. Steganografia. Kryptografia (Wprowadzenie. Komponenty szyfrów współczesnych. Szyfry blokowe. Szyfry strumieniowe. Szyfry wykładnicze. Funkcje skrótu - integralność danych. Podpis cyfrowy i PKI. Uwierzytelnianie podmiotów. Niezaprzeczalność. Zarządzanie kluczami. Kontrola dostępu za pomocą haseł.). Bezpieczeństwo w sieciach komputerowych (uwierzytelnianie w warstwie dostępowej: PAP, CHAP, EAP; SSH, bezpieczna poczta elektroniczna-PGP; SSL/TLS, HTTPS; IPsec, sieci wirtualne). Standardy oceny bezpieczeństwa. Etyka komputerowa.

Ćwiczenia laboratoryjne obejmują: Zajęcia organizacyjne ? tematyka ćwiczeń, zasady zaliczenia, podstawowa terminologia. Implementacja prostych szyfrów. Kryptoanaliza szyfrów prostych. Badanie jakości szyfratorów blokowych w różnych trybach pracy i porównanie czasów szyfrowania i deszyfrowania różnych algorytmów. Badanie jakości wybranych funkcji skrótu. Publiczny system kryptograficzny ? PGP. Kryptografia asymetryczna.

Literatura podstawowa:

1. Wprowadzenie do kryptografii (Introduction to Cryptography), Buchmann J. A., Wydawnictwo Naukowe PWN (Springer), Warszawa (New York), 2006 (2004

2. Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Stokłosa J. (red.), Wydawnictwo Politechniki Poznańskiej, Poznań, 2005

3. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001

Literatura uzupełniająca:

1. Kryptografia (Cryptography. Theory and Practice), Stinson D.R., WNT (CRC Press), Warszawa (Boca Raton), 2005 (1995)

2. Kryptografia w praktyce, Ferguson N., Schneier B., Helion, Gliwice, 2004

3. Firewalle i bezpieczeństwo w sieci, Chestwick W. R. , Bellovin S.M. , Rubin A.D., Helion, Gliwice, 2003

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Wykłady	30
2. Ćwiczenia laboratoryjne	30
3. Bieżące przygotowanie do ćwiczeń laboratoryjnych	30
4. Przygotowanie sprawozdań z laboratoriów	15
5. Przygotowanie do sprawdzianu	15
6. Przygotowanie do egzaminu	20
7. Udział w konsultacjach i egzaminie	10

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	150	6
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	70	3
Zajęcia o charakterze praktycznym	70	3