

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Ochrona danych		Kod 1010334491010330124
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) (brak)	Rok / Semestr 5 / 9
Ścieżka obieralności/specjalność Bezpieczeństwo systemów informatycznych	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: I stopień	Forma studiów (stacjonarna/niestacjonarna) niestacjonarna	
Godziny Wykłady: - Ćwiczenia: - Laboratoria: 8 Projekty/seminaria: 8		Liczba punktów 3
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 %) 3 100%

Odpowiedzialny za przedmiot / wykładowca: 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

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 oraz podstaw ochrony danych
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 poszerzenie umiejętności stosowania metod ochrony danych w systemach informatycznych.

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

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

Projekt zalicza się na podstawie obecności, wykonanego projektu i dokumentacji do projektu.

Treści programowe

<p>Ćwiczenia laboratoryjne</p> <p>Implementacja szyfrów. Kryptoanaliza szyfrów. 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.</p>		
<p>Projekt</p> <p>Opracowanie projektu w zakresie bezpieczeństwa danych.</p>		
<p>Literatura podstawowa:</p> <ol style="list-style-type: none"> 1. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001 2. Wprowadzenie do kryptografii (Introduction to Cryptography), Buchmann J. A., Wydawnictwo Naukowe PWN (Springer), Warszawa (New York), 2006 (2004) 3. Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Stokłosa J. (red.), Wydawnictwo Politechniki Poznańskiej, Poznań, 2005 4. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001 5. Wprowadzenie do kryptografii (Introduction to Cryptography), Buchmann J. A., Wydawnictwo Naukowe PWN (Springer), Warszawa (New York), 2006 (2004) 6. Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Stokłosa J. (red.), Wydawnictwo Politechniki Poznańskiej, Poznań, 2005 		
<p>Literatura uzupełniająca:</p> <ol style="list-style-type: none"> 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. Firewallle i bezpieczeństwo w sieci, Chestwick W. R. , Bellovin S.M. , Rubin A.D., Helion, Gliwice, 2003 4. Kryptologia. Budowa i łamanie zabezpieczeń, Wobst R., Wydawnictwo RM, Warszawa, 2002 5. Kryptografia (Cryptography. Theory and Practice), Stinson D.R., WNT (CRC Press), Warszawa (Boca Raton), 2005 (1995) 6. Kryptografia w praktyce, Ferguson N., Schneier B., Helion, Gliwice, 2004 7. Firewallle i bezpieczeństwo w sieci, Chestwick W. R. , Bellovin S.M. , Rubin A.D., Helion, Gliwice, 2003 8. Kryptologia. Budowa i łamanie zabezpieczeń, Wobst R., Wydawnictwo RM, Warszawa, 2002 		
<p>Bilans nakładu pracy przeciętnego studenta</p>		
<p>Czynność</p>		<p>Czas (godz.)</p>
1. Udział w zajęciach projektowych		8
2. Udział w ćwiczeniach laboratoryjnych		8
3. Praktyczne przygotowanie do ćwiczeń laboratoryjnych		13
4. Przygotowanie sprawozdań z laboratoriów		18
5. Wykonanie projektu		30
6. Udział w konsultacjach		8
<p>Obciążenie pracą studenta</p>		
<p>forma aktywności</p>	<p>godzin</p>	<p>ECTS</p>
Łączny nakład pracy	85	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	35	1
Zajęcia o charakterze praktycznym	75	3