

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Podstawy ochrony danych</b>		Kod <b>1010334561010334967</b>
Kierunek studiów <b>Informatyka</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>(brak)</b>	Rok / Semestr <b>3 / 6</b>
Ścieżka obieralności/specjalność <b>-</b>	Przedmiot oferowany w języku: <b>polski</b>	Kurs (obligatoryjny/obieralny) <b>obligatoryjny</b>
Stopień studiów: <b>I stopień</b>	Forma studiów (stacjonarna/niestacjonarna) <b>niestacjonarna</b>	
Godziny Wykłady: <b>20</b> Ćwiczenia: <b>-</b> Laboratoria: <b>16</b> Projekty/seminaria: <b>-</b>		Liczba punktów <b>5</b>
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) <b>(brak)</b>		(ogólnouczelniany, z innego kierunku) <b>(brak)</b>
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki <b>nauki techniczne</b>		Podział ECTS (liczba i %) <b>5 100%</b>

#### 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	<b>Wiedza:</b>	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	<b>Umiejętności:</b>	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	<b>Kompetencje społeczne</b>	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. Śluz 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:**

**Literatura uzupełniająca:**

**Bilans nakładu pracy przeciętnego studenta**

<b>Czynność</b>	<b>Czas (godz.)</b>	
1. Wykłady	20	
2. Ćwiczenia laboratoryjne	16	
3. Bieżące przygotowanie do ćwiczeń laboratoryjnych	20	
4. Przygotowanie sprawozdań z laboratoriów	10	
5. Przygotowanie do sprawdzianu	10	
6. Przygotowanie do egzaminu	10	
7. Udział w konsultacjach i egzaminie	4	
<b>Obciążenie pracą studenta</b>		
<b>forma aktywności</b>	<b>godzin</b>	<b>ECTS</b>
Łączny nakład pracy	90	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	40	3
Zajęcia o charakterze praktycznym	40	3