

**WYDZIAŁ INFORMATYKI I ZARZĄDZANIA PWR  
KARTA PRZEDMIOTU**

**Nazwa w języku polskim: Bezpieczeństwo i ochrona danych**  
**Nazwa w języku angielskim: Computer Security and Data Protection**  
**Kierunek studiów (jeśli dotyczy): Informatyka**  
**Stopień studiów i forma: I stopień, niestacjonarna**  
**Rodzaj przedmiotu: obowiązkowy**  
**Kod przedmiotu: INZ004113**  
**Grupa kursów: NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	18		9		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	30		60		
Forma zaliczenia	zaliczenie na ocenę		Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	1		2		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,4		0,8		

\*niepotrzebne skreślić

**WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI**

1. Podstawowa wiedza z zakresu analizy i algebry
2. Podstawowa wiedza z zakresu sieci informatycznych

**CELE PRZEDMIOTU**

C1 Nabycie podstawowej wiedzy, uwzględniającej jej aspekty aplikacyjne, z zakresu współczesnej kryptografii i ochrony danych.  
 C2. Zdobywanie umiejętności wyboru i stosowania odpowiednich metod ochrony danych.  
 C3. Nabywanie i utrwalanie kompetencji społecznych obejmujących inteligencję emocjonalną polegającą na umiejętności współpracy w grupie studenckiej mającej na celu efektywne rozwiązywanie problemów. Odpowiedzialność, uczciwość i rzetelność w postępowaniu; przestrzeganie obyczajów obowiązujących w środowisku akademickim i społeczeństwie.

### PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy:

PEK\_W01 Posiada wiedzę z zakresu współczesnej kryptografii

PEK\_W02 Zna podstawowe atrybuty bezpieczeństwa danych

Z zakresu umiejętności:

PEK\_U01 Potrafi rozróżniać klasy algorytmów kryptograficznych

PEK\_U02 Potrafi dobrać odpowiednie metody dla ochrony wybranego atrybutu bezpieczeństwa danych

PEK\_U03 Potrafi ocenić poziom ochrony danych w systemie informatycznym w kontekście wykorzystanych metod kryptograficznych

Z zakresu kompetencji społecznych:

PEK\_K01 Rozumie potrzebę ciągłego doskonalenia się w zakresie bezpieczeństwa systemów informatycznych

PEK\_K02 Rozumie rolę kryptografii w procesie zapewnienia wysokiego poziomu bezpieczeństwa w społeczeństwie informacyjnym

### TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie: bezpieczeństwo w systemach informatycznych	2
Wy2	Historyczne algorytmy kryptograficzne, elementy kryptoanalizy klasycznych algorytmów szyfrowania	2
Wy3	Blokowe algorytmy szyfrowania, elementy kryptoanalizy blokowych algorytmów szyfrowania	2
Wy4	Kryptografia asymetryczna	2
Wy5	Kryptograficzne funkcje skrótu i ich zastosowania	2
Wy6	Ataki na kryptograficzne funkcje skrótu .	2
Wy7	Ataki na kryptograficzne algorytmy asymetryczne	2
Wy8	Praktyczne zastosowania kryptografii	2
Wy8	Test wiedzy	2
Suma godzin		<b>18</b>

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
Suma godzin		

Forma zajęć - laboratorium		Liczba godzin
La1	Zajęcia organizacyjne	1
La2	Klasyczne algorytmy kryptograficzne	2
La3	Blokowe algorytmy kryptograficzne	2
La4	Asymetryczne algorytmy szyfrowania	2
La5	Podpis elektroniczny	2
Suma godzin		<b>9</b>

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
Pr4		
...		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
...		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1. Wykład tradycyjny N2. Praca własna – przygotowanie do laboratoriów i opracowanie wyników eksperymentów N3. Ćwiczenia laboratoryjne - wykorzystanie oprogramowania edukacyjnego N4. Konsultacje dla zainteresowanych studentów N5. Praca własna – samodzielne studia i przygotowanie do testu wiedzy	

#### OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru))	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEK_W01- PEK_W02, PEK_U01- PEK_U03, PEK_K01- PEK_K02,	Sprawozdania z wykonanych ćwiczeń laboratoryjnych, odpowiedzi ustne dotyczące realizowanych ćwiczeń
P PEK_W01- PEK_W02, Test końcowy		

<b>LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA</b>	
<b><u>LITERATURA PODSTAWOWA:</u></b>	
[1]	Stallings, William , Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii / Gliwice : Helion, cop. 2012.
[2]	Schneier, Bruce, Kryptografia dla praktyków : protokoły i programy źródłowe w języku C / Warszawa : Wydawnictwa Naukowo-Techniczne, 2002.
[3]	Menezes, Alfred J. Kryptografia stosowana / Warszawa : Wydawnictwa Naukowo-Techniczne, 2005.
<b><u>LITERATURA UZUPEŁNIAJĄCA:</u></b>	
[1]	Kapczyński, Adrian. Kryptografia kwantowa i biometria jako rozwinięcie klasycznych metod ochrony informacji / Gliwice : Wydawnictwo Politechniki Śląskiej, [2009]
[2]	Kahn, David, Łamacze kodów : historia kryptologii / Warszawa : Wydawnictwa Naukowo-Techniczne, 2004.
[3]	Wobst, Reinhard, Kryptologia : budowa i łamanie zabezpieczeń / Warszawa : Wydawnictwo RM, 2002.
<b>OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)</b>	
<b>Grzegorz Kołaczek, Grzegorz.Kolaczek@pwr.wroc.pl</b>	

**MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU**  
**Bezpieczeństwo i ochrona danych**  
**Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU Informatyka**

<b>Przedmiotowy efekt kształcenia</b>	<b>Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**</b>	<b>Cele przedmiotu***</b>	<b>Treści programowe***</b>	<b>Numer narzędzia dydaktycznego***</b>
<b>PEK_W01 (wiedza)</b>	K1INF_W13	C1	Wy2-Wy8	N1,N4-N5
<b>PEK_W02</b>	K1INF_W13	C1	Wy1,W8	N1,N5
<b>PEK_U01 (umiejętności)</b>	K1INF_U09	C2	Wy1-Wy8 La1-La5	N2-N4
<b>PEK_U02</b>	K1INF_U03, K1INF_U09	C2,C3	Wy1-Wy8 La1-La5	N2-N4
<b>PEK_U03</b>	K1INF_U09, K1INF_U14	C2,C3	Wy1-Wy8 La1-La5	N2-N4
<b>PEK_K01 (kompetencje)</b>	K1INF_U09	C1,C3	Wy1,La1-La5	N4,N5
<b>PEK_K02</b>	K1INF_W13	C1,C2,C3	Wy8,La1-La5	N4,N5

\*\* - wpisać symbole kierunkowych/specjalnościowych efektów kształcenia

\*\*\* - z tabeli powyżej