WYDZIAŁ INFORMATYKI I ZARZĄDZANIA PWR

KARTA PRZEDMIOTU

Nazwa w języku polskim: Bezpieczeństwo systemów
Nazwa w języku angielskim: Systems Security
Kierunek studiów (jeśli dotyczy): Informatyka
Specjalność (jeśli dotyczy): Teleinformatyka
Stopień studiów i forma: II stopień, stacjonarna
Rodzaj przedmiotu: obowiązkowy
Kod przedmiotu INZ003807
Grupa kursów NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			30	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	120			30	
Forma zaliczenia	zaliczenie na ocenę			zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**4**			1	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0			1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	2,4			0,6	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1. Podstawowa wiedza z zakresu sieci informatycznych
2. Podstawowa wiedza z zakresu kryptografii

\

CELE PRZEDMIOTU

C1 Nabycie podstawowej wiedzy odnośnie metod szacowania ryzyka oraz z zakresu norm i metod projektowania systemów bezpieczeństwa dla instytucji.
C2. Zdobycie umiejętności dotyczących wypracowania strategii wyboru zabezpieczeń oraz zasad tworzenia architektury bezpieczeństwa.
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 zarządzania bezpieczeństwem informacji i usług.

PEK_W02 Posiada wiedzę z zakresu obowiązujących norm i standardów dotyczących bezpieczeństwa teleinformatycznego.

PEK_W03 Zna metody analizy i zarządzania ryzykiem w teleinformatyce.

Z zakresu umiejętności:

PEK_U01 Potrafi zaprojektować architekturę bezpieczeństwa dla systemu teleinformatycznego wybranej instytucji.

PEK_U02 Potrafi określić wymagania dotyczące zabezpieczeń i strategii bezpieczeństwa.

PEK_U03 Potrafi dokonać analizy ryzyka w systemach teleinformatycznych.

Z zakresu kompetencji społecznych:

PEK_K01 Rozumie potrzebę identyfikacji ryzyka w systemach teleinformatycznych

PEK_K02 Rozumie rolę polityki bezpieczeństwa w kształtowaniu poziomu bezpieczeństwa systemów teleinformatycznych stanowiących podstawę społeczeństwa informacyjnego.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do tematyki bezpieczeństwa systemów teleinformatycznych.	2
Wy2	Wprowadzenie do zarządzania bezpieczeństwem informacji i usług	2
Wy3	Normy, standardy i zalecenia	2
Wy4	Ryzyko w sensie ogólnym i technicznym	2
Wy5	Analiza ryzyka i strategie zarządzania nim w teleinformatyce	2
Wy6	Wybrane metody i komputerowe narzędzia wspomagające analizę ryzyka.	2
Wy7	Trójpoziomowy model hierarchii celów, strategii i polityki	2
Wy8	System bezpieczeństwa instytucji	2
Wy9	Wysokopoziomowa (ogólna) analiza ryzyka i wyznaczenie obszarów wymagających ochrony	2
Wy10	Przebieg szczegółowej analizy ryzyka w systemach teleinformatycznych	2
Wy11	Wzorce wymagań dotyczących zabezpieczeń	2
Wy12	Wypracowanie strategii wyboru zabezpieczeń	2
Wy13	Ogólne zasady tworzenia architektury bezpieczeństwa i dobór zabezpieczeń na podstawie zdefiniowanych wymagań	2
Wy14	Polityka bezpieczeństwa teleinformatycznego	2
Wy15	Test wiedzy	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		

..		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1		
La2		
La3		
La4		
La5		
…		
	Suma godzin	

Forma zajęć - projekt		Liczba godzin
Pr1	Zajęcia organizacyjne. Przedstawienie i omówienie zagadnień projektowych.	2
Pr2	Zdefiniowanie celu i określenie zadań dla wybranych zagadnień projektowych.	2
Pr3	Przegląd literatury dla wybranych zagadnień projektowych.	2
Pr4	Specyfikacja algorytmów, metod, narzędzi potrzebnych do realizacji wybranych zagadnień projektowych.	2
Pr5	Raport bieżący z postępów prac projektowych.	2
Pr6	Plan eksperymentów oraz ewaluacji rozwiązania.	2
Pr7	Dokumentacja prac projektowych.	2
Pr8	Opis rozwiązania– instrukcja developera (architektura, założenia, diagram klas)	2
Pr9	Opis rozwiązania – instrukcja użytkownika oraz udostępniane funkcjonalności.	2
Pr10	Raport bieżący z postępów prac projektowych.	2
Pr11	Badania jakościowe opracowanego rozwiązania	2
Pr12	Badania ilościowe opracowanego rozwiązania	2
Pr13	Ocena osiągniętej funkcjonalności i wyników badań.	2
Pr14	Określenie możliwości rozwoju opracowanego rozwiązania.	2
Pr15	Podsumowanie i przegląd rezultatów otrzymanych w trakcie realizacji projektu.	2
	Suma godzin	**30**

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

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1.Wykład tradycyjny N2. Praca własna – przygotowanie projektu . N3. Zajęcia projektowe – metodyka pracy nad projektem.

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_W03, PEK_U01- PEK_U03, PEK_K01- PEK_K02,	Sprawozdania z wykonanych zadań w ramach zajęć projektowych, prezentacje postępów prac projektowych.
P PEK_W01- PEK_W02, Test końcowy		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Białas, Andrzej. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie / Andrzej Białas. Warszawa : Wydawnictwo Naukowo-Techniczne, cop. 2007.

[2] Zalewski, Michal , Cisza w sieci : praktyczny przewodnik po pasywnym rozpoznawaniu i atakach pośrednich / Gliwice : Helion, cop. 2005

[3] Księżopolski, Bogdan , Audyt bezpieczeństwa systemów IT-ścieżka techniczna (rekonesans i skanowanie) / Lublin : Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2011

LITERATURA UZUPEŁNIAJĄCA:

[1] RASH M., OREBAUGH A., CLARK G., PINKARD B., BABBIN J.,IPS. Zapobieganie i aktywne przeciwdziałanie intruzom, wyd. MIKOM 2005

[2] MOLSKI M., ŁACHETA M., Przewodnik audytora systemów informatycznych, wyd. Helion 2006

[3] Zalewski, Michal, Splątana sieć. Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW, Helion, cop. 2012

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Grzegorz Kołaczek, Grzegorz.Kolaczek@pwr.wroc.pl

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Bezpieczeństwo Systemów
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU **Informatyka**
I SPECJALNOŚCI **Teleinformatyka**

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**	Cele przedmiotu***	Treści programowe***	Numer narzędzia dydaktycznego***
PEK_W01 (wiedza)	K2INF_W04, K2INF_W06 K2INF_W06_S2TEL_W05	C1	Wy1,Wy2 Wy7,Wy8, Wy11-Wy13	N1,N4-N5
PEK_W02	K2INF_W06_S2TEL_W05	C1	Wy1-Wy3,Wy14	N1,N5
PEK_W03	K2INF_W06, K2INF_W06_S2TEL_W05	C1	Wy4- Wy6, Wy9, Wy10	N1,N5
PEK_U01 (umiejętności)	K2INF_U08_S2TEL_U07	C2,C3	Wy13 ,Pr2-Pr14	N2-N4
PEK_U02	K2INF_U07, K2INF_U08_S2TEL_U04	C2,C3	Wy11-Wy12, Pr2-Pr14	N2-N4
PEK_U03	K2INF_U08_S2TEL_U03	C1,C2	Wy4-Wy6,Wy9,Wy10 Pr2-Pr14	N2-N4
PEK_K01 (kompetencje)	K2INF_U08_S2TEL_U07	C3	Wy4-Wy6,Wy9,Wy10, Pr2-Pr14	N1,N4,N5
PEK_K02	K2INF_U08_S2TEL_U07	C3	Wy1-Wy2,Wy14, Pr2-Pr14	N1,N4,N5

** - wpisać symbole kierunkowych/specjalnościowych efektów kształcenia
*** - z tabeli powyżej