WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa w języku polskim: Wytwarzanie bezpiecznych aplikacji
Nazwa w języku angielskim: Programming secure applications
Kierunek studiów (jeśli dotyczy): Informatyka
Specjalność (jeśli dotyczy): Bezpieczeństwo i niezawodność systemów informatycznych
Stopień studiów i forma: ~~I~~ / II stopień*, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: ~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ *
Kod przedmiotu INZ003824WL
Grupa kursów ~~TAK~~ / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	90		60		
Forma zaliczenia	Zaliczenie na ocenę		Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	3		2		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		1		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1,8		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1. Wiedza i kompetencje z zakresu programowania przynajmniej w dwóch językach spośród C#, Java, PHP, HTML/XML z JavaScript, Python.
2. Znajomość tworzenia aplikacji w jednej spośród technologii PHP, JSP, ASP lub jednej platformie spośród XAMP/WAMP, J2EE, MS Visual Studio, dowolny system CMS, lub w dowolnym frameworku tworzenia aplikacji internetowych i systemów oprogramowania.
3. Wiedza i kompetencje z zakresu baz danych i języka SQL.

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy o metodach tworzenia bezpiecznego kodu programów i aplikacji w różnych językach programowania i na różnych platformach wytwarzania oprogramowania.
C2 Nabycie wiedzy z zakresu programistycznych mechanizmów zabezpieczania danych w bazach oraz programowania bezpiecznych aplikacji i serwisów sieciowych.
C3 Nabycie wiedzy mechanizmach programistycznych wzmacniania bezpieczeństwa programów, aplikacji i serwisów internetowych.

C4 Nabycie zaawansowanej wiedzy o mechanizmach, bibliotekach i komponentach do programowania systemów kryptograficznych na platformach programistycznych i deweloperskich aplikacji internetowych i systemów informatycznych.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy student:

PEK_W01 – posiada wiedzę o wytwarzaniu bezpiecznego kodu i bezpiecznych aplikacji w językach programowania Java, C#, na platformach JSP, ASP.NET i oraz w języku C/C++.

PEK_W02 – ma wiedzę o programowaniu i wytwarzaniu bezpiecznych aplikacji na różnych platformach i w różnych środowiskach i językach wolnego oprogramowania – w tym PHP, Python, Joomla!, Drupal, WAMP, XAMP i różnych środowiskach wytwarzania systemów CMS.

PEK_W03 – posiada wiedzę o przeciwdziałaniu zagrożeniom aplikacji webowych i systemów od mechanizmów programistycznych.

PEK_W04 – zna mechanizmy bezpieczeństwa platform technologicznych i deweloperskich J2EE/SE, PHP, ASP.NET, AJAX, środowiskach WAMP i XAMP, oraz Python, Joomla!, Drupal do projektowania systemów CMS.

PEK_W05 – zna mechanizmy bezpieczeństwa serwerów internetowych i bazodanowych.

Z zakresu umiejętności student:

PEK_U01 – potrafi wytwarzać bezpieczny kod programów w różnych językach programowania.

PEK_U02 – potrafi korzystać z mechanizmów wytwarzania bezpiecznych aplikacji internetowych i systemów na platformie JSP. Umie usuwać podatności i testować zabezpieczenia.

PEK_U03 – potrafi korzystać z mechanizmów wytwarzania bezpiecznych aplikacji internetowych i systemów na platformach ASP.NET. Umie usuwać podatności i testować zabezpieczenia.

PEK_U04 – potrafi korzystać z mechanizmów wytwarzania bezpiecznych aplikacji internetowych i systemów na platformach wolego oprogramowania i wytwarzania systemów CMS – PHP, Joomla!, Python, Drupal. Umie usuwać podatności i testować zabezpieczenia.

PEK_U05 – potrafi tworzyć zabezpieczania dostępności systemów informatycznych i serwisów internetowych.

PEK_U06 – potrafi zaimplementować aplikację internetową lub niewielki systemu o wzmocnionym bezpieczeństwie w wybranym języku programowania w wybranej technologii i na wybranej platformie deweloperskiej.

PEK_U07 (nowy!) – ma przygotowanie niezbędne do pracy w pracowniach komputerowych i zna zasady bezpieczeństwa związane z tą pracą. Stosuje te zasady również do infrastruktury i serwisów webowych dostępnych z komputerów w pracowniach komputerowych.

Z zakresu kompetencji społecznych student:

PEK_K01 – rozumie znaczenie bezpieczeństwa informatycznych systemów i serwisów

internetowych dla procesów ekonomicznych, społecznych oraz bezpieczeństwa państwa i społeczeństwa.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do wytwarzania bezpiecznego kodu. Tworzenie bezpiecznych aplikacji w języku C/C++. Tworzenie bezpiecznych aplikacji w języku C#. Bezpieczne komponenty dla platformy Java.	2
Wy2	Programowanie bezpiecznych aplikacji technologii PHP i CMS Joomla!. Zagrożenia bezpieczeństwa w systemach zarządzania bazami danych.	2
Wy3	Programowanie aplikacji webowych z zabezpieczeniami przeciw atakom generowania, pobierania i wykonywania złośliwego kodu. Przeciwdziałanie zagrożeniom pochodzącym od mechanizmów programistycznych – bezpieczeństwo struktur wskaźnikowych oraz wycieki pamięci – awarie programów i systemów.	2
Wy4	Programowanie aplikacji odpornych na ataki przepełniania stosu przy wykonywaniu kodu – wykonywanie złośliwego kodu i odmowa usług.	2
Wy5	Mechanizmy bezpieczeństwa na platformach programistycznych. Programowanie systemów kryptograficznych na platformach technologicznych JSP, PHP, w systemach CMS.	2
Wy6	Mechanizmy programistyczne bezpieczeństwa na platformach technologicznych ASP.NET i AJAX. Mechanizmy bezpiecznego dostępu do danych – programowanie bezpiecznych aplikacji i serwisów oraz mechanizmy serwerów internetowych i bazodanowych.	2
Wy7	Zabezpieczanie operatywności usług i systemów informatycznych poprzez filtrowanie ruchu sieciowego, równoważenie obciążenia, mechanizmów klasteryzacji oraz zapewnienia jakości usług (QoS). Kolokwium zaliczeniowe.	2
Wy8	Podsumowanie wykładu. Zaliczenia.	1
	Suma godzin	**15**

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

	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1	Zasady wytwarzania bezpiecznego kodu – studialne przykłady praktyczne. Omówienie tematyki studenckich prac badawczych, sposobu studiowania tematów, przygotowania dokumentacji z badań i prezentacji. Akwizycja tematów prac badawczych.	2
La2	Tworzenie bezpiecznych aplikacji w języku C/C++ - przykłady praktyczne. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La3	Bezpieczne programy dla platformy Java – przykłady studialne. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La4	Tworzenie aplikacji w języku C# - usuwanie podatności, testowanie zabezpieczeń. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La5	Programowanie bezpiecznych aplikacji technologii PHP i CMS Joomla!. Wykorzystywanie bezpiecznych, dobrze przetestowanych komponentów Joomla! i skryptów PHP. Mechanizmy zabezpieczeń dostępu do baz danych MySQL i PostgreSQL. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La6	Zagrożenia bezpieczeństwa i mechanizmy zabezpieczeń w systemach zarządzania bazami danych MySQL, PostgreSQL i MS SQL Server. Przykłady praktyczne tworzenia aplikacji z zabezpieczeniem dostępu do baz danych na różnych platformach developerskich. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La7	Programowanie aplikacji webowych z zabezpieczeniami przeciw atakom generowania, pobierania i wykonywania złośliwego kodu. Przykłady praktyczne zabezpieczonych aplikacji WWW – tworzenie lub uruchamianie i testowanie. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La8	Mechanizmy bezpiecznego dostępu do danych – programowanie bezpiecznych aplikacji i serwisów oraz mechanizmy serwerów internetowych i sieciowych – przykłady praktyczne na platformach developerskich ASP.NET/Visual Studio, JSP/J2EE, PHP, CMS Joomla!, platformach serwerowych IIS, Apache Tomcat, Apache. Praktyczne ćwiczenia z zakresu dwóch studenckich prac badawczych.	2
La9	Przeciwdziałanie zagrożeniom pochodzącym od mechanizmów programistycznych – bezpieczeństwo struktur wskaźnikowych oraz wycieki pamięci – awarie programów i systemów. Przykłady praktyczne programów w językach C/C++, C#, Java, PHP. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La10	Programowanie aplikacji odpornych na ataki przepełniania stosu przy wykonywaniu kodu – wykonywanie złośliwego kodu i odmowa usług. Przykłady praktyczne programów w językach C/C++, C#, Java, PHP. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La11	Mechanizmy bezpieczeństwa na platformach programistycznych. Szczegółowa analiza na platformie Visual Studio, J2EE, CMS Joomla!. Praktyczne ćwiczenia z zakresu studenckich prac	2

	badawczych.	
La12	Programowanie systemów kryptograficznych. Programowanie niewielkich systemów kryptografii symetrycznej, niesymetrycznej oraz funkcji skrótu do szyfrowania i podpisywania. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La13	Mechanizmy programistyczne bezpieczeństwa na platformach technologicznych .NET i AJAX. Zaawansowane mechanizmy i przykłady kodu. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La14	Mechanizmy programistyczne bezpieczeństwa na platformach technologicznych J2EE, PHP, CMS Joomla!. Przykłady tworzenia bezpiecznych witryn, portali i systemów biznesowych i informacyjnych. Analiza przykładów systemów biznesowych o bezpiecznych architekturach z zastosowaniem Web Services ze specjalizowanym stosem protokołów bezpiecznego dostępu do usług sieciowych. Praktyczne ćwiczenia z zakresu studenckich prac badawczych.	2
La15	Praktyczne rozwiązania zabezpieczania dostępności usług i systemów informatycznych poprzez filtrowanie ruchu sieciowego, równoważenie obciążenia, mechanizmów klasteryzacji oraz zapewnienia jakości usług (QoS), oparte na specjalizowanych serwerach. Analiza i testowania przykładowego rozwiązania. Praktyczne ćwiczenia z zakresu studenckich prac badawczych. Zaliczenia.	2
	Suma godzin	30

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 oparty o prezentacje multimedialne. N2. Laboratorium komputerowe z dostępem do Internetu i z możliwością wirtualizacji stacji roboczych i serwerów. N3. Praca własna studentów – udział w realizacji studenckich prac badawczych i zadań laboratoryjnych. N4. Praca własna – samodzielne studiowanie problematyki wykładu.

N5. Konsultacje dla studentów.

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_U06	Ocena za wykonanie i dokumentację aplikacji internetowej o wzmocnionym bezpieczeństwie.
F2	PEK_U01-PEK_U05	Oceny za wykonanie i dokumentację zadań laboratoryjnych.
P	PEK_W01-PEK_W05	Kolokwium na wykładzie.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] L. Powers, M. Snell, *Microsoft Visual Studio 2008. Księga eksperta*, Helion, Gliwice, 2009.
[2] E. Jendrock, I. Evans, D. Gollapudi, K. Haase, Ch. Srivathsa, *Java EE 6. Przewodnik. Wydanie IV*, Helion, Gliwice, 2012.
[3] H. Schildt, *Java. Kompendium programisty. Wydanie VIII*, Helion, Gliwice, 2012.
[4] J. Ross, *Bezpieczne programowanie. Aplikacje hakeroodporne*, Helion, Gliwice, 2009.
[5] L. Ullman, *E-commerce. Genialnie proste tworzenie serwisów w PHP i MySQL*, Helion, Gliwice, 2011.
[6] B. Hoffman, B. Sullivan, *Bezpieczeństwo aplikacji tworzonych w technologii Ajax*, Helion, Gliwice, 2009.
[7] T. Canavan, *Joomla! Zabezpieczanie witryn*, Helion, Gliwice, 2010.
[8] D. Overton, *Small Business Server 2008 PL. Instalacja, migracja i konfiguracja*, Helion, Gliwice, 2010.

LITERATURA UZUPEŁNIAJĄCA:

[1] C. Shiflett, *PHP. Bezpieczne programowanie*, Helion, Gliwice, 2006.
[2] C.S. Horstmann, G. Cornell, *Java. Techniki zaawansowane. Wydanie VIII*, Helion, Gliwice, 2009.
[3] M. Hall, L. Brown, Y. haikin, *Core Java Servlets i JavaServer Pages. Tom II. Wydanie II*, Helion, Gliwice, 2009.
[4] J. Viega, M. Messier, *C i C++. Bezpieczne programowanie, Receptury*, Helion, Gliwice, 2005.

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

doc. dr inż. Jacek Gruber, 71 320 33 40; jacek.gruber@pwr.wroc.pl

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Wytwarzanie bezpiecznych aplikacji
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU Informatyka
I SPECJALNOŚCI Bezpieczeństwo i niezawodność systemów informatycznych

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_W02-K2INF_W06	C1, C4	Wy1	N1, N3-N5
PEK_W02	K2INF_W02-K2INF_W06	C1-C4	Wy2	N1, N3-N5
PEK_W03	K2INF_W02-K2INF_W06	C1-C4	Wy3-Wy4, Wy7	N1, N3-N5
PEK_W04	K2INF_W02-K2INF_W06	C2-C4	Wy5	N1, N3-N5
PEK_W05	K2INF_W02-K2INF_W06	C1-C4	Wy6	N1, N3-N5
PEK_U01 (umiejętności)	K2INF_W07	C1, C4	La2	N2-N5
PEK_U02	K2INF_U06-K2INF_U07	C2-C4	La3, La8-La14	N2-N5
PEK_U03	K2INF_U06-K2INF_U07	C2-C4	La3, La8-La14	N2-N5
PEK_U04	K2INF_U06-K2INF_U07	C1-C4	La5-La6	N2-N5
PEK_U05	K2INF_U06-K2INF_U07	C2-C4	La5-La14	N2-N5
PEK_U06	K2INF_U06-K2INF_U07	C1-C4	La1-La15	N2-N5
PEK_U07 nowy!	K2INF_U09	C1-C4	Lab1	C1-C4
PEK_K01 (kompetencje)	K2INF_W02-K2INF_W06	C2-C4	Wy1-Wy8	N1-N5

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