Zał. nr 4 do ZW 33/2012

WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa w języku polskim: Zaawansowane systemy bezpieczeństwa informatycznego
Nazwa w języku angielskim: Advanced information security systems
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 INZ003826WL
Grupa kursów ~~TAK~~ / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	90		90		
Forma zaliczenia	Zaliczenie na ocenę		Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	3		3		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		1,5		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1,8		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1. Wiedza i kompetencje z zakresu przedmiotu Bezpieczeństwo sieciowe i internetowe.
2. Wiedza i kompetencje z zakresu przedmiotu Modele niezawodności systemów informatycznych.
3. Podstawowa znajomość statystyki matematycznej.

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy w zakresie zaawansowanej inżynierii bezpieczeństwa systemów informatycznych.
C2 Nabycie wiedzy o zaawansowanych metodach i mechanizmach bezpieczeństwa informatycznej infrastruktury procesów biznesowych oraz o bezpieczeństwie chmury obliczeniowej.
C3 Nabycie wiedzy o systemach zapobiegania i wykrywania zagrożeń IDS i IPS oraz o systemach wykrywania nadużyć FD.
C4 Nabycie podstawowej wiedzy o kwantowych systemach kryptograficznych.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy student:

PEK_W01 – ma rozszerzoną wiedzę o koncepcji bezpieczeństwa systemów i sieci, złożonych mechanizmach poufności, uwierzytelniania, autoryzacji i integralności informacji w procesach biznesowych i informacyjnych i w złożonej infrastrukturze informatycznej.

PEK_W02 – posiada rozszerzoną wiedzę o wadach kryptografii klasycznej, wadach klasycznej infrastruktury PKI.

PEK_W03 – ma wiedzę o zaawansowanych metodach i mechanizmach bezpieczeństwa informatycznej infrastruktury procesów biznesowych oraz o bezpieczeństwie chmury obliczeniowej.

PEK_W04 – ma zawansowaną wiedzę o zagrożeniach systemu systemów operacyjnych, komunikacji i protokołów komunikacyjnych, ma podstawową wiedzę o kwantowych systemach kryptograficznych.

PEK_W05 – ma wiedzę o systemach zapobiegania i wykrywania zagrożeń IDS i IPS oraz o systemach wykrywania nadużyć FD.

PEK_W06 – ma wiedzę o zagrożeniach od rozproszonych słowników, od baz i repozytoriów wiedzy o kluczach i hasłach w systemach kryptograficznych, ma wiedzę o zapobieganiu utracie danych i przywracaniu systemów po awarii, a także normach i standardach de facto audytów bezpieczeństwa.

Z zakresu umiejętności student:

PEK_U01 – potrafi ocenić jakość i oceniać i stosować narzędzia do monitoringu w miejscach pracy, stosować zaawansowane mechanizmy i rozwiązania bezpieczeństwa sieci bezprzewodowych.

PEK_U02 – potrafi stosować i zarządzać mechanizmami bezpieczeństwa serwerów systemowych, sieciowych i internetowych, przeprowadzać ich audyt, wykorzystywać zaawansowane mechanizmy bezpieczeństwa portali społecznościowych i komunikatorów, stosować narzędzia do testowania zabezpieczeń serwisów webowych.

PEK_U03 – potrafi stosować narzędzia i testy wykrywające defekty oprogramowania, systemy wykrywania nadużyć bankowych, wykrywać ruch sieciowy wskazujący na wykorzystywanie sieci TOR, zapobiegać zagrożeniom od zaawansowanej socjotechniki.

PEK_U04 – potrafi stosować metody i narzędzia do oceny ryzyka, posługiwać się w stopniu podstawowym infrastrukturą kryptografii kwantowej, zbudować serwerową infrastrukturę PKI, budować systemy i środowiska firewall, stroić i wykorzystywać mechanizmy bezpieczeństwa aplikacji.

PEK_U05 – 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 ze stacji roboczych w pracowniach komputerowych.

Z zakresu kompetencji społecznych student:

PEK_K01 – rozumie znaczenie bezpieczeństwa systemów informatycznych i internetowych w przebiegu procesów społecznych i ekonomicznych.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Koncepcja bezpieczeństwa systemów i sieci.	2
Wy2	Cechy informacji bezpiecznej. Klasyfikacja zagrożeń i podatności.	2
Wy3	Poufność informacji, uwierzytelnianie, autoryzacja, integralność.	2
Wy4	Klasyczna kryptografia i kryptoanaliza - algorytmy symetryczne i asymetryczne i funkcje skrótów.	2
Wy5	Wady generyczne kryptografii klasycznej.	2
Wy6	Infrastruktura PKI, standard X509 – zalety i wady generyczne.	2
Wy7	Podstawy kryptografii kwantowej. Kwantowe systemy kryptograficzne.	2
Wy8	Ataki na system operacyjny. Podatności na ataki.	2
Wy9	Ataki na komunikację i protokoły komunikacyjne. Inteligentne zapory i filtry sieciowe.	2
Wy10	Bezpieczeństwo aplikacji i usług Web, usług sieciowych, poczty elektronicznej, komunikatorów. Bezpieczeństwo baz danych. Bezpieczeństwo chmury obliczeniowej.	2
Wy11	Architektury i protokoły bezpieczeństwa aplikacji biznesowych oparte o usługi sieciowe Web Services.	2
Wy12	Inteligentne polityki bezpieczeństwa i zarządzanie bezpieczeństwem. Inteligentne systemy wykrywania i zapobiegania atakom, systemy IDS i IPS. Systemy detekcji nadużyć i naruszeń w systemach i aplikacjach biznesowych.	2
Wy13	Rozproszone słowniki, bazy i repozytoria wiedzy o kluczach i hasłach w systemach kryptograficznych.	2
Wy14	Zapobieganie utracie danych i przywracanie systemów po awarii.	2
Wy15	Rozproszone systemy audytu, ataków i wzmacniania bezpieczeństwa. Współczesne normy i standardy audytów bezpieczeństwa. Kolokwium zaliczeniowe.	2
	Suma godzin	**30**

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

Forma zajęć - laboratorium		Liczba godzin
La1	GIODO - Generalny Inspektor Ochrony Danych Osobowych. Monitoring w miejscach pracy. Aplikacje TotalView, Surfcontrol, Cyberpatrol, Surfwatch i umocowanie prawne.	2
La2	Bezpieczeństwo baz danych pod kontrolą różnych serwerów DBMS.	2
La3	Bezpieczeństwo sieci Wi-Fi i WiMAX. Standard 802.16. Zaawansowane mechanizmy i rozwiązania Wi-Fi i WiMAX. Dostawcy i routery WiMAX. Wykorzystanie serwerów zdalnej autoryzacji - RADIUS.	2
La4	Bezpieczeństwo sieci firmowej z wykorzystaniem mechanizmów	2

	bezpieczeństwa Microsoft Windows Server. Monitorowanie i audyt serwerów usług internetowych.	
La5	Portale społecznościowe a prawo. Mechanizmy bezpieczeństwo portali społecznościowych Facebook i Google+. Bezpieczeństwo komunikatorów. Dostrajanie i testowanie bezpieczeństwa.	2
La6	Narzędzia testowania funkcjonalnego serwisów internetowych - Sahi, Webdriver, Selenium RC.	2
La7	Predykcja defektów oprogramowania – modele i metryki, testowanie.	2
La8	Systemy data mining do wykrywania nadużyć w aplikacjach bankowych i biznesowych.	2
La9	Bezpieczeństwo informacji w sieci rozproszonej TOR oraz kryptowaluta Bitcoin.	2
La10	Ataki na bezpieczeństwo sieci, systemów i portali z wykorzystaniem zaawansowanej socjotechniki.	2
La11	Metody i narzędzia oceny ryzyka - OCTAVE, CRAMM, MARION, MEHARI.	2
La12	Kryptografia kwantowa – fundamentalnie bezpieczna infrastruktura generowania i dostarczania kluczy kryptograficznych.	2
La13	PKI – dostawcy w Polsce. PKI – serwery certyfikatów.	2
La14	Bezpieczny firewall. Przegląd i konfiguracja środowiska Forefront TMG 2010.	2
La15	Bezpieczeństwo w Ruby on Rails – przykład bezpiecznej aplikacji WWW. Zaliczenia.	2
	Suma godzin	

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 zadań laboratoryjnych. N4. Praca własna – samodzielne studiowanie problematyki wykładu i przygotowanie do kolokwium zaliczeniowego. 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_U01-PEK_U04, PEK_K01	Oceny za wykonanie i dokumentację prac badawczych.
F2	PEK_U01-PEK_U04, PEK_K01	Oceny za wykonanie i dokumentację zadań laboratoryjnych.
P	PEK_W01-PEK_W06	Kolokwium zaliczeniowe z wykładu.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] S. Weerawarana, F. Curbera, F. Leymann, T. Storey, D.F. Ferguson, *Web Services Platform Architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and More*, Prentice Hall, 2005.

[2] Z. Fryźlewicz, D. Nikończuk, Windows Azure. *Wprowadzenie do programowania w chmurze*, Helion, Gliwice 2012.

[3] A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion, Gliwice 2012.

[4] D. Biesiada, T. Kopacz, A. Żarski, P. Cichocki, B. Zass, M. Żyliński, *Windows Azure. Platforma Cloud Computing dla programistów*, APN Promise, Gliwice, Warszawa 2010.

[5] W. Jacak (i in.), *Wstęp do Informatyki i Kryptografii Kwantowej*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011.

LITERATURA UZUPEŁNIAJĄCA:

[1] G. Bahadur, J. Inasi, Alex de Carvalho, *Securing the Clicks Network Security in the Age of Social Media*, McGraw-Hill Companies, 2011.

[2] M. Harwood, M. Goncalves, M. Pemble, *Security Strategies in Web Applications and Social Networking*, *Security Strategies in Web Applications and Social Networking*, Jones & Bartlett Learning, 2011.

[3] T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, Addison-Wesley Professional, 2007.

[4] M. Maliński, *Weryfikacja hipotez statystycznych wspomagana komputerowo*, Wyd. Politechniki Śląskiej, Gliwice 2004.

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
Zaawansowane systemy bezpieczeństwa informatycznego
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_W03, K2INF_W06, K2INF_U05	C1-C2	Wy4	N1, N3-N5
PEK_W02	K2INF_W03, K2INF_W06	C1-C2	Wy1-Wy2	N1, N3-N5
PEK_W03	K2INF_W03, K2INF_W06, K2INF_U05	C1-C2	Wy4-Wy5	N1, N3-N5
PEK_W04	K2INF_W03, K2INF_W06, K2INF_U05	C1,C4	Wy3	N1, N3-N5
PEK_W05	K2INF_W03, K2INF_W06, K2INF_U05	C1-C2	Wy6	N1, N3-N5
PEK_W06	K2INF_W03, K2INF_W06, K2INF_U05	C1,C3	Wy7-Wy15	N1, N3-N5
PEK_U01 (umiejętności)	K2INF_W03, K2INF_W06, K2INF_U05	C1-C2	La1	N2-N5
PEK_U02	K2INF_W03, K2INF_W06, K2INF_U05	C1-C3	La2	N2-N5
PEK_U03	K2INF_U05	C1-C2	La3-La5	N2-N5
PEK_U04	K2INF_W03, K2INF_W06, K2INF_U05	C1,C2	La6-La15	N2-N5
PEK_U05	K2INF_U09	C1-C4	La1-La15	N2-N4
PEK_K01 (kompetencje)	K2INF_W03, K2INF_W06, K2INF_U05	C1-C4	Wy1-Wy15, La1-La15	N5

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