Zał. nr 4 do ZW 33/2012

WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa w języku polskim: Bezpieczeństwo sieciowe i internetowe
Nazwa w języku angielskim: Network and Internet security
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 INZ003960
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)	85		90		
Forma zaliczenia	Egzamin		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		3		
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 sieci komputerowych.
2. Wiedza i kompetencje z zakresu baz danych i języka SQL.
3. Umiejętność administrowania systemów operacyjnych Windows i Linux.
4. Znajomość języków i platform programowania aplikacji internetowych (HTML, XML, C#, JavaScript).

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy z zakresu inżynierii bezpieczeństwa systemach sieciowych i internetowych, bezpieczeństwa stosu protokołów TCP/IP i stosu protokołów Web Services.
C2 Nabycie wiedzy o metodach zabezpieczania integralności danych, ochrony sieci za pomocą zapór sieciowych i systemów IDS oraz IPS do wykrywania i zapobiegania atakom.
C3 Nabycie wiedzy o mechanizmach i narzędziach do podwyższania bezpieczeństwa oraz polityki i audytu bezpieczeństwa systemów i sieci oraz bezpieczeństwa procesów informacyjnych i biznesowych.
C4 Zdobycie umiejętności stosowania narzędzi, metod, mechanizmów i rozwiązań

programowych do podwyższania bezpieczeństwa, audytu bezpieczeństwa oraz tworzenia systemów wykrywania ataków.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy student:

PEK_W01 – posiada wiedzę o koncepcja bezpieczeństwa systemów i sieci, o cechach informacji bezpiecznej, zna klasyfikację ataków na bezpieczeństwo systemów i sieci.

PEK_W02 – posiada wiedzę o bezpieczeństwie sieci i stosu protokołów TCP/IP, ma wiedzę o atakach na komunikację, protokoły i infrastrukturę IP, DNS i usług katalogowych, oraz przeciwdziałaniu tym atakom, ma wiedzę z zagrożeniach i realizacjach ataków DoS i DDoS oraz o mechanizmach obrony systemów i sieci przed tymi atakami, posiada wiedzę o inteligentnych systemach IDS i IPS wykrywania i zapobiegania atakom, oraz o systemach FD.

PEK_W03 – ma wiedzę o bezpieczeństwie sieci WiFi i WiMAX, zna standardy i protokoły bezpiecznej komunikacji bezprzewodowej.

PEK_W04 – ma wiedzę o bezpieczeństwie internetowych systemów informacyjnych i usługowych oraz zagrożeniach i zabezpieczeniach przed atakami SQL Injection i XSS, WWW, poczty elektronicznej, komunikatorów, wyszukiwarek, infrastruktury Web Services, procesów biznesowych, chmury obliczeniowej.

PEK_W05 – posiada wiedzę atakach socjotechnicznych, Phishingu oraz o zapobieganiu tym atakom, a także bezpieczeństwie bankowości elektronicznej, posiada zaawansowaną wiedzę o usługach i infrastrukturze PKI – realizacjach hierarchii certyfikacji, od centrów certyfikacji do serwerowych usług certyfikacji.

PEK_W06 – ma wiedzę o polityce bezpieczeństwa systemów informatycznych i sieciowych, oraz wiedzę o audycie bezpieczeństwa – różnych jego modelach, metodykach, standardach, a także standardach de facto i najlepszych praktykach.

Z zakresu umiejętności student:

PEK_U01 – potrafi ocenić jakość i stosować narzędzia do testów penetracyjnych oraz skanery bezpieczeństwa systemów i sieci.

PEK_U02 – potrafi demonstrować scenariusze ataków oraz badać i stosować metody i narzędzia wykrywania i zapobiegania atakom i wzmacniania bezpieczeństwa systemów, sieci i serwisów webowych.

PEK_U03 – potrafi stosować zabezpieczenia biometryczne.

PEK_U04 – potrafi wykonać audyt bezpieczeństwa informatycznego za pomocą wybranych metodyk i narzędzi.

Z zakresu kompetencji społecznych student:

PEK_K01 – rozumie znaczenie bezpieczeństwa informatycznego, procesów społecznych i biznesowych, oraz informatycznych systemów narodowych, rządowych i samorządowych.

PEK_K02 – umie pracować zespołowo nad zadaniami studialnymi i wdrażać rozwiązania.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Koncepcja bezpieczeństwa systemów i sieci.	2
Wy2	Cechy informacji bezpiecznej. Klasyfikacja ataków.	2
Wy3	Poufność informacji, uwierzytelnianie, autoryzacja, integralność.	2
Wy4	Podstawowy kryptografii, szyfrowanie symetryczne i asymetryczne. Infrastruktura PKI, standard X509.	2
Wy5	Kryptografia w systemach i sieciach.	2
Wy6	Bezpieczeństwo sieci i stosu protokołów TCP/IP.	2
Wy7	Ataki na system operacyjny – wirusy, robaki, ukryte kanały komunikacyjne.	2
Wy8	Ataki na komunikację i protokół IP, architektury zapór sieciowych, translacja adresów i filtry pakietów.	2
Wy9	Bezpieczeństwo aplikacji i usług sieciowych – WWW, poczty elektronicznej, komunikatorów, wyszukiwarek sieciowych, infrastruktury WEB services, obrona przed XSS i SQL Injection.	2
Wy10	Bezpieczeństwo bankowości elektronicznej.	2
Wy11	Bezpieczeństwo usług katalogowych. Bezpieczeństwo sieci bezprzewodowych.	2
Wy12	Uwierzytelnianie i kontrola dostępu w sieciach intranetowych i korporacyjnych.	2
Wy13	Polityka bezpieczeństwa, standardy i normy.	2
Wy14	IDS i IPS wykrywania i zapobiegania atakom.	2
Wy15	Audyt bezpieczeństwa.	2
	Suma godzin	**30**

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

Forma zajęć - laboratorium		Liczba godzin
La1	Bezpieczeństwo stosu protokołów TCP/IP.	2
La2	Ataki DoS i zapobieganie. Łamanie haseł.	2
La3	Narzędzia testów penetracyjnych. Skanery bezpieczeństwa systemów i sieci.	2
La4	Sniffing – metody i narzędzia. Wykrywanie i zapobieganie.	2
La5	IP Spoofing. ARP Spoofing. Ataki Man-In-The-Middle i zapobieganie.	2
La6	DNS spoofing i zapobieganie.	2
La7	Wykrywanie i zabezpieczenia przed działaniem programów malware.	2
La8	Ataki XSS i zapobieganie. Ataki SQL Injection i zapobieganie.	2
La9	Ataki na zabezpieczenia WEP, WPA, WPA2. Bezpieczeństwo infrastruktury sieci bezprzewodowych.	2
La10	Sprzętowe i programowe systemy Firewall.	2
La11	Certyfikacja i infrastruktura PKI. Certyfikaty informacyjnych i	

	biznesowych serwisów www, poczty elektronicznej, serwerów i klientów usług webowych i poczty. PGP i GPG.	
La12	Ataki socjotechniczne. Phishing i zapobieganie. Google Hacking.	2
La13	Zabezpieczenia biometryczne.	2
La14	Bezpieczeństwo komunikatorów i portali społecznościowych, systemów ze stosem protokołów usług Web Services, chmury obliczeniowej, procesów biznesowych. Symulacja ataku w kryptografii kwantowej.	2
La15	Audyt bezpieczeństwa. Narzędzia i systemy audytu. 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 zadań laboratoryjnych. N4. Praca własna – samodzielne studiowanie problematyki wykładu i przygotowanie do egzaminu. 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_U02 PEK_K02	Oceny za wykonanie i dokumentację prac badawczych.
F2	PEK_U01, PEK_U03-PEK_U04,	Oceny za wykonanie i dokumentację zadań laboratoryjnych.
P	PEK_W01-PEK_W06	Egzamin.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] R. Anderson, *Inżynieria zabezpieczeń*, WNT, Warszawa 2005.
[2] B. Schneider, *Kryptografia dla praktyków. Protokoły, algorytmu i programy źródłowe w języku C*, WNT, Warszawa 2002.
[3] E. Cole, R. Krutz, J. Conley, *Bezpieczeństwo sieci. Biblia*, Helion, Gliwice 2005.
[4] J. Pieprzyk, T. Hardjono, J. Seberry, *Teoria bezpieczeństwa systemów komputerowych*, Helion, Gliwice 2005.
[5] A. Lockhart, *125 sposobów na bezpieczeństwo sieci*, Helion, Gliwice 2007.
[6] B. Smith, B. Komar, *MS Windows Security Resorce Kit*, Microsoft Press, 2003.
[7] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej firmie*, WNT, Warszawa 2007.
[8] M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.
[9] ISACA. *Standardy, wytyczne i procedury audytowania i kontrolowania systemów informatycznych*, 2002.

LITERATURA UZUPEŁNIAJĄCA:

[1] K. Lidermann, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Helion, Gliwice, 2003.
[2] T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006.
[3] S. Garfinkel, G. Stafford, *WWW. Bezpieczeństwo i handel*, Helion, Gliwice 1999.
[4] B. Toxen, *Bezpieczeństwo w Linuxie – Podręcznik administratora*, Helion, 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
Bezpieczeństwo sieciowe i internetowe
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_W01	C1	Wy1-Wy3	N1, N3-N5
PEK_W02	K2INF_W01-K2INF_W02, K2INF_W04, K2INF_W06	C1-C2, C4	Wy6-Wy8, Wy11, Wy14	N1, N3-N5
PEK_W03	K2INF_W02, K2INF_W06	C2	Wy11-Wy12	N1, N3-N5
PEK_W04	K2INF_W02-K2INF_W06	C2-C3,	Wy9, Wy11-Wy12	N1, N3-N5
PEK_W05	K2INF_W02-K2INF_W06	C1-C4	Wy-Wy5, Wy10-Wy12	N1, N3-N5
PEK_W06	K2INF_W03-K2INF_W06	C1-C4	Wy8-Wy9, Wy13-Wy15	N1, N3-N5
PEK_U01 (umiejętności)	K2INF_06, K2INF_U09	C1-C4	La1-La14	N2-N5
PEK_U02	K2INF_U06-K2INF_U07	C1-C2	La1-La2, La4, La8-La9, La14	N2-N5
PEK_U03	K2INF_U09	C1-C4	La1-La15	N2-N5
PEK_U04	K2INF_U06, K2INF_U09	C1-C4	La2-La13	N2-N5
PEK_K01 (kompetencje)			Wy1-Wy15	N5
PEK_K02			La1-La15	N1-N5

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