

**WYDZIAŁ INFORMATYKI I ZARZĄDZANIA PWR****KARTA PRZEDMIOTU****Nazwa w języku polskim: Inżynieria bezpieczeństwa systemów****Nazwa w języku angielskim: Network and Internet Systems Security Engineering****Kierunek studiów (jeśli dotyczy): Informatyka****Stopień studiów i forma: I stopień, stacjonarna****Rodzaj przedmiotu: wybieralny****Kod przedmiotu: INZ005229****Grupa kursów: NIE**

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

\*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 Nabywanie podstawowej wiedzy, uwzględniającej jej aspekty aplikacyjne, z zakresu analizy i projektowania systemów bezpieczeństwa.

C2. Zdobycie umiejętności wyboru i stosowania odpowiednich metod oceny i gwarantowania poziomu bezpieczeństwa systemów teleinformatycznych.

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 metod oceny i gwarantowania poziomu bezpieczeństwa systemów teleinformatycznych

PEK\_W02 Zna podstawowe elementy planu bezpieczeństwa

Z zakresu umiejętności:

PEK\_U01 Potrafi scharakteryzować kolejne fazy planu bezpieczeństwa

PEK\_U02 Potrafi wskazać odpowiednie metody i mechanizmy wspierające realizację celów danej fazy planu bezpieczeństwa

PEK\_U03 Potrafi korzystać z podstawowych narzędzi oceny i zapewniania poziomu bezpieczeństwa systemów teleinformatycznych

Z zakresu kompetencji społecznych:

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

PEK\_K02 Rozumie rolę planu bezpieczeństwa dla zapewnienia bezpieczeństwa teleinformatycznego w społeczeństwie informacyjnym

### TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie. Cele planu bezpieczeństwa.	2
Wy2	Faza I planu bezpieczeństwa. Inspekcja	2
Wy3	Faza II planu bezpieczeństwa. Ochrona systemów i sieci teleinformatycznych.	2
Wy4	Faza III planu bezpieczeństwa. Wykrywanie problemów bezpieczeństwa.	2
Wy5	Faza IV planu bezpieczeństwa. Reagowanie.	2
Wy6	Faza V planu bezpieczeństwa. Refleksja.	2
Wy7	Bezpieczeństwo w sieci Internet – podatności protokołów komunikacyjnych	2
Wy8	Bezpieczeństwo w sieci Internet – protokół IPSec i IPv6	2
Wy9	Bezpieczeństwo w sieci Internet – protokół SSL/TLS oraz SSH	2
Wy10	Infrastruktura klucza publicznego	2
Wy11	Bezpieczeństwo sieci bezprzewodowych	2
Wy12	Metody wykrywania intruzów i anomalii	2
Wy13	Narzędzia wykrywania intruzów i anomalii	2
Wy14	Bezpieczeństwo aplikacji	2
Wy15	Test wiedzy	2
	Suma godzin	<b>30</b>

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

<b>Forma zajęć - laboratorium</b>		<b>Liczba godzin</b>
La1	Zajęcia wprowadzające. Konfiguracja środowiska.	2
La2	Bezpieczeństwo poczty elektronicznej – pakiet GnuPGP	2
La3	Steganografia	2
La4	Bezpieczeństwo haseł	2
La5	Skanowanie systemów komputerowych	2
La6	Analiza ruchu sieciowego	2
La7	Ataki ARP-spoofing	2
La8	Ataki DNS-spoofing	2
La9	Ataki na sesje SSL/TLS	2
La10	Testy penetracyjne	2
La11	Prywatność w sieciach publicznych – TOR	2
La12	Sieci VPN	2
La13	Systemy pułapki - Honeypot	2
La14	Infrastruktura klucza publicznego	2
La15	Podsumowanie wykonanych ćwiczeń	2
	Suma godzin	<b>30</b>

<b>Forma zajęć - projekt</b>		<b>Liczba godzin</b>
Pr1		
Pr2		
Pr3		
Pr4		
...		
	Suma godzin	

<b>Forma zajęć - seminarium</b>		<b>Liczba godzin</b>
Se1		
Se2		
Se3		
...		
	Suma godzin	

<b>STOSOWANE NARZĘDZIA DYDAKTYCZNE</b>	
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**

<b>Oceny</b> (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru))	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEK_W01- PEK_W02,	Sprawozdania z wykonanych ćwiczeń laboratoryjnych, odpowiedzi ustne dotyczące

	PEK_U01- PEK_U03, PEK_K01- PEK_K02,	realizowanych ćwiczeń
P PEK_W01- PEK_W02, Test końcowy		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA	
<p><b><u>LITERATURA PODSTAWOWA:</u></b></p> <p>[1] Liderman, Krzysztof. Analiza ryzyka i ochrona informacji w systemach komputerowych / Warszawa : Wydawnictwo Naukowe PWN : Mikom, 2008.</p> <p>[2] Pipkin, Donald L. Bezpieczeństwo informacji : ochrona globalnego przedsiębiorstwa / Warszawa : Wydawnictwa Naukowo-Techniczne, 2002</p> <p>[3] Bishop, Matt. Computer security : art and science / Boston : Addison-Wesley, cop. 2003.</p> <p><b><u>LITERATURA UZUPEŁNIAJĄCA:</u></b></p> <p>[1] Metasploit : the penetration tester's guide / San Francisco : No Starch Press, cop. 2011.</p> <p>[2] Księżopolski, Bogdan , Audyt bezpieczeństwa systemów IT-ścieżka techniczna (rekonesans i skanowanie) / Lublin : Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2011.</p> <p>[3] Surmacz, Tomasz Robert. Secure systems and networks / Wrocław : Wrocław University of Technology ; Łódź : PRINTPAP, 2011.</p>	
<b>OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)</b>	
Grzegorz Kołaczek, Grzegorz.Kolaczek@pwr.wroc.pl	

**MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU**  
**Inżynieria bezpieczeństwa systemów**  
**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_W04	C1	Wy7-Wy14 La5-La13	N1,N4-N5
<b>PEK_W02</b>	K1INF_W04	C1	Wy1-Wy6	N1,N5
<b>PEK_U01 (umiejętności)</b>	K1INF_W04, K1INF_U06, K1INF_U13	C2	Wy1-Wy6	N2-N4
<b>PEK_U02</b>	K1INF_W04, K1INF_U06, K1INF_U13	C2,C3	La2-La14	N2-N4
<b>PEK_U03</b>	K1INF_W04, K1INF_U06, K1INF_U07, K1INF_U13	C2,C3	Wy11,Wy13, Wy14,La10- La14	N2-N4
<b>PEK_K01 (kompetencje)</b>	K1INF_U06	C1,C3	Wy1-Wy14 La1-La14	N1,N4,N5
<b>PEK_K02</b>	K1INF_U13	C1,C2,C3	Wy1-Wy6	N1,N4,N5

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

\*\*\* - z tabeli powyżej