UNIWERSYTET MORSKI W GDYNI
Wydział Przedsiębiorczości i Towaroznawstwa

KARTA PRZEDMIOTU

Kod przedmiotu		Nazwa przedmiotu	w jęz. polskim	**BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH**
			w jęz. angielskim	**INFORMATION SYSTEM SECURITY**

Kierunek	**Innowacyjna Gospodarka**
Specjalność	**Informatyka Gospodarcza**
Poziom kształcenia	**studia pierwszego stopnia**
Forma studiów	**stacjonarne**
Profil kształcenia	**ogólnoakademicki**
Status przedmiotu	**obowiązkowy**
Rygor	**egzamin**

Semestr studiów	Liczba punktów ECTS	Liczba godzin w tygodniu				Liczba godzin w semestrze			
		W	C	L	P	W	C	L	P
V	4	2		1		30		15	
Razem w czasie studiów						**45**			

Wymagania w zakresie wiedzy, umiejętności i innych kompetencji
Brak wymagań wstępnych.

Cele przedmiotu
Zapoznanie studenta z istotą bezpieczeństwa, bezpieczeństwa informacyjnego, problematyką bezpieczeństwa systemu informacyjnego (SI) oraz technologii towarzyszących jak: kontrola wewnętrzna, audyt, CAAT's. Ukształtowanie podstawowych umiejętności z zakresu obsługi systemów bezpieczeństwa SI.

Osiągane efekty uczenia się dla przedmiotu (EKP)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
EKP_01	wymienia, objaśnia i klasyfikuje pojęcia zakresu bezpieczeństwa i polityki bezpieczeństwa SI.	NK_W06, NK_U02
EKP_02	ma wiedzę o standardach polityki bezpieczeństwa w odniesieniu do SI.	NK_W06, NK_U02
EKP_03	potrafi wykorzystać standardy oceny polityki bezpieczeństwa SI (technologie i standardy audytu bezpieczeństwa).	NK_W06, NK_U02
EKP_04	ma świadomość celów i zasad organizowania pracy zespołu projektującego, wdrażającego i eksploatującego system bezpieczeństwa SI.	NK_U14, NK_K05
EKP_05	ma podstawowe umiejętności z zakresu ochrony SI w odniesieniu do współczesnych technologii informatycznych (ochrona dostępu, uwierzytelnianie, analiza antywirusowa, zapory, itd.).	NK_U02, NK_U07, NK_U08

Treści programowe	Liczba godzin				Odniesienie do EKP
	W	C	L	P	
Kształtowania polityki bezpieczeństwa systemu informacyjnego (SI) (wartość systemu informacyjnego; wartość informacji, sprzętu, oprogramowania, rodzaj i zakres potencjalnych zagrożeń oraz koszt strat wynikających z tych zagrożeń, koszt szkolenia personelu obsługującego system, zakres ochrony fizycznej (zewnętrznej) i programowo-sprzętowej (wewnętrznej), itd. Kontrola wewnętrzna i audyt bezpieczeństwa.	4				EKP_01, EKP_02, EKP_03, EKP_04
Standardy bezpieczeństwa: TCSEC (Trusted Computer Security Evaluation Criteria – Orange Book), ITSEC (Information Technology Security Evaluation Criteria). Polska Norma PN-I-13335-1 - „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.” PN-ISO/IEC TR 13335-3 – „Techniki zarządzania bezpieczeństwem systemów informatycznych”.	2				EKP_01, EKP_02, EKP_03, EKP_04
Bezpieczeństwo systemu informacyjnego (SI). Podmioty bezpieczeństwa informacyjnego w SI: dane, oprogramowanie, sprzęt informatyczny, dokumentacje (archiwa, kopie), użytkownicy.	6				EKP_01, EKP_02, EKP_03, EKP_04
Bezpieczeństwo baz danych i SZBD. Poufność, integralność, nadmiarowość i współbieżność. Technologie identyfikacji, uwierzytelniana, autoryzacji. Upoważnienia.	6				EKP_01, EKP_02, EKP_04
Technologie szyfrowania i steganografia.	2				EKP_01, EKP_02, EKP_04
Zagrożenia sieciowe. Klasyfikacje zagrożeń sieciowych (wg CERT). Instytucje NASK, CERT, CERN. Istota hakingu. Programy niszczące i szpiegujące. Spam. Technologie ochrony sieciowej-zapory sieciowe. Zagrożenia w sieciach bezprzewodowych (standardy 802.11 i inne).	2				EKP_01, EKP_02, EKP_04
Audyt informatyczny, technologie audytu informatycznego. ISACA i jej produkty. COBIT.	6				EKP_01, EKP_02, EKP_03, EKP_04
Technologie CAAT’s. Rynek aplikacji CAAT’s.	2				EKP_01, EKP_02, EKP_03, EKP_04
Identyfikacja stanu komputera – audyt zasobów, identyfikacja systemu.			1		EKP_01, EKP_02, EKP_05
Identyfikacja i klasyfikacja zagrożeń dla systemu komputera, przykłady ataków.			1		EKP_01, EKP_02, EKP_05
Podstawy bezpieczeństwa w systemie – ochrona dostępu na poziomie użytkownika.			1		EKP_01, EKP_02, EKP_05
Udostępnianie zasobów systemu.			1		EKP_01, EKP_02, EKP_05
Ochrona systemu metodami kryptografii.			1		EKP_01, EKP_02, EKP_05
Bezpieczeństwo usług sieciowych na przykładzie serwera WWW.			2		EKP_01, EKP_02, EKP_05
Ochrona systemów – zapory, detekcja zagrożeń, prewencja.			2		EKP_01, EKP_02, EKP_05
Ochrona obiegu dokumentów - kryptografia, certyfikaty.			2		EKP_01, EKP_02, EKP_05
Instytucje zajmujące się bezpieczeństwem – przegląd wybranych serwisów.			1		EKP_01, EKP_02, EKP_05
Polityka bezpieczeństwa informacji – przykłady.			1		EKP_01, EKP_02, EKP_05
Zadanie podsumowujące – implementacja przykładowej polityki bezpieczeństwa w wybranym systemie.			2		EKP_01, EKP_02, EKP_05
Łącznie godzin	**30**		**15**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol EKP	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
EKP_01			X						
EKP_02			X						
EKP_03			X						
EKP_04			X						
EKP_05								X	

Kryteria zaliczenia przedmiotu
Egzamin pisemny (test=10 pytań testowych). Próg zaliczenia 60%. Zaliczenie laboratorium, zadanie zliczające. Próg zaliczający 75%. Zaliczenie przedmiotu: pozytywna ocena z laboratorium i pozytywna ocena z egzaminu.

Uwaga: student otrzymuje ocenę powyżej dostatecznej, jeżeli uzyskane efekty uczenia się przekraczają wymagane minimum.

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	30		15	
Czytanie literatury	15		10	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			15	
Przygotowanie do egzaminu, zaliczenia	15			
Opracowanie dokumentacji projektu/sprawozdania				
Uczestnictwo w zaliczeniach i egzaminach	2			
Udział w konsultacjach	2		2	
Łącznie godzin	**64**		**42**	
Sumaryczna liczba godzin dla przedmiotu	**106**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**4**			
	Liczba godzin		**ECTS**	
Obciążenie studenta związane z zajęciami praktycznymi	42		2	
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	51		2	

Literatura podstawowa
Pipkin D. L.. Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa. WNT. Warszawa 2002. Żółkiewicz J. Materiały do wykładu „Bezpieczeństwo systemów informacyjnych". AMG. ILIAS. Gdynia 2018, 2019.
Literatura uzupełniająca
Fisher B. Przestępstwa komputerowe i ochrona informacji. Kantor Wydawniczy Zakamycze 2000. Kraków. Harley d., R. Slade, U. E. Gattiker. Wirusy cała prawda. Wydawnictwo Translator. Warszawa 2003. Liderman K. Analiza ryzyka i ochrona informacji. MIKOM-PWN. Warszawa 2008. Polaczek T. Audyt Bezpieczeństwa Informacji W Praktyce. Helion. Gliwice 2006. Scambray J., S. McClure, G. Kurtz. Hakerzy - cała prawda. Wydawnictwo Translator. Warszawa 2001. Schetina E., K. Green, J. Carlson. Bezpieczeństwo w sieci. Helion. Gliwice 2002. Strebe M. Bezpieczeństwo sieci. Mikom 2005.

Osoba odpowiedzialna za przedmiot	
dr inż. Janusz Żółkiewicz	KSI
Pozostałe osoby prowadzące przedmiot	
mgr Ireneusz Meyer	KSI
mgr inż. Henryk Szreder	KSI