KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: **ZAGROŻENIA W SYSTEMACH INFORMACYJNYCH**		*Kod przedmiotu:* **KNS/BW-IIP/BC/56**
Nazwa przedmiotu w języku angielskim: **THREATS TO INFORMATION SYSTEMS**		
Kierunek studiów: **Bezpieczeństwo wewnętrzne**	*Profil:* **praktyczny**	*Poziom studiów:* **II stopień**
Specjalność/specjalizacja: **Bezpieczeństwo cyberprzestrzeni**	*Forma zaliczenia przedmiotu:* **egzamin**	*Semestr studiów:* **4**
Nazwa grupy zajęć: **zajęcia specjalnościowe**	*Język w jakim prowadzone są zajęcia:* **polski**	

Tryb studiów	*Forma zajęć*							*Ogólna liczba godzin*	*Liczba punktów ECTS:*
	W	*Ćw.*	*Konw.*	*Lab.*	*Proj.*	*Sem.*	*Zajęcia terenowe*		
Tryb stacjonarny	**15**	**-**	**-**	**-**	**15**	**-**	**-**	**30**	**4**
Tryb niestacjonarny	**15**	**-**	**-**	**-**	**9**	**-**	**-**	**24**	

Jednostka realizująca przedmiot, wydział:
Kolegium Nauk Społecznych

Odpowiedzialny za opracowanie karty przedmiotu (tytuł/stopień naukowy, imię i nazwisko, adres e-mail):
dr inż. Stefan Senczyna, ssenczyna@wszop.edu.pl

CEL PRZEDMIOTU

C1.	Poznanie przez studentów zagrożeń wynikających z korzystania z systemów informatycznych, w tym instrumentów płatniczych on-line.
C2.	Zapoznanie studentów ze specyfiką różnego rodzaju ataków na systemy informacyjne – zdalnych oraz z wykorzystaniem fizycznego dostępu i metodami zabezpieczania się przed nimi.
C3.	Kształtowanie wiedzy o słabych i silnych stronach bezpieczeństwa systemów informatycznych.

WYMAGANIA WSTĘPNE

1.	Podstawy użytkowania systemu Windows
2.	Podstawowa wiedza o funkcjach systemów informacyjnych
3.	Wyszukiwanie informacji w Internecie

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ		METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ	ODNIESIENIE DO:	
			TREŚCI PROGRAMOWYCH	KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ
EU1	Student ma wiedzę z zakresu zagrożeń systemów informacyjnych potrzebną dla przeciwdziałania	egzamin pisemny (pytania otwarte) zadania projektowe	W1, W2 P2	BW K_W 05
EU2	Student zna rodzaje i zasady funkcjonowania ataków na systemy informacyjne i jest świadomy zagrożeń, jakie za sobą niosą.	egzamin pisemny (pytania otwarte) zadania projektowe	W3 P1	BW K_W 07
EU3	Student potrafi rozróżnić rodzaje ataków na systemy informacyjne i przeciwdziałać nim.	egzamin pisemny (pytania otwarte) zadania projektowe	W4, W5 P1-P3	BW K_U 03

TREŚCI PROGRAMOWE

L.p.	WYKŁAD	Liczba godzin	
		S	N
W1	Wprowadzenie do problematyki bezpieczeństwa systemów komputerowych Podstawowe definicje i problemy Bezpieczeństwo systemów komputerowych. Zagrożenia. Ataki. Ryzyko. Luka (vulnerability). Środki ochrony (controls) Ogólne własności bezpieczeństwa informacji Poufność (confidentiality). Integralność (integrity). Dostępność (availability). Autentyczność (authenticity). Niezaprzeczalność (non-repudiation). Kontrola dostępu (access control) Problemy i wyzwania w bezpieczeństwie systemów komputerowych Zarządzanie tożsamością i dostępem. Ochrona danych. Ochrona przed malware. Bezpieczeństwo sieci. Zarządzanie incydentami. Edukacja użytkowników	3	3
W2	Bezpieczeństwo poczty elektronicznej Zagrożenia i problemy związane z pocztą elektroniczną Phishing. Malware. Spam. Sniffing i przechwytywanie danych Mechanizmy ochrony poczty elektronicznej Szyfrowanie. Filtrowanie antyspamowe i antywirusowe. Autoryzacja nadawców. Bezpieczne hasła i uwierzytelnianie dwuskładnikowe (2FA) Polityka bezpieczeństwa Cele polityki bezpieczeństwa Składniki polityki bezpieczeństwa	3	3
W3	Destrukcja systemu operacyjnego Przyczyny i skutki destrukcji systemu operacyjnego Ochrona przed destrukcją systemu operacyjnego	3	3
W4	Bezpieczeństwo Internetu Uwarunkowania bezpieczeństwa Złożoność i różnorodność środowiska internetowego: Dynamicznie zmieniające się zagrożenia: Brak jednolitych standardów bezpieczeństwa: Globalny zasięg i anonimowość: Ludzki czynnik	3	3
W5	Metody zapewnienia bezpieczeństwa systemów informacyjnych. Ochrona fizyczna (kontrola dostępu, monitoring, zabezpieczenia przeciwpożarowe i przeciwwodne), ochrona techniczna, ochrona organizacyjna (polityka bezpieczeństwa, szkolenia pracowników, zarządzanie incydentami bezpieczeństwa, kopie zapasowe), ochrona użytkownika	3	3
	RAZEM	**15**	**15**

FORMA I KRYTERIA ZALICZENIA WYKŁADU: egzamin pisemny (pytania otwarte) - ocena ilościowa

L.p.	**PROJEKT**	**Liczba godzin**	
		S	**N**
P1	Analiza przypadku naruszenia bezpieczeństwa w znanej firmie. Identyfikacja luk w zabezpieczeniach, które doprowadziły do ataku, oraz propozycja rozwiązania, które mogłyby zapobiec podobnym incydentom w przyszłości.	5	3
P2	Opracowanie słownika terminów związanych z bezpieczeństwem systemów komputerowych. Słownik powinien zawierać definicje najważniejszych pojęć, przykłady oraz ilustracje.	5	3
P3	Opracowanie prezentacji, która porównuje różne modele bezpieczeństwa informacji (np. model CIA, model Biba). Prezentacja powinna zawierać szczegółowy opis każdego modelu oraz porównanie ich zalet i wad.	5	3
	RAZEM	**15**	**9**

FORMA I KRYTERIA ZALICZENIA PROJEKTU: zadania projektowe - ocena jakościowa

METODY I FORMY DYDAKTYCZNE

1.	wykład informacyjny
2.	wykład problemowy
3.	praca grupowa
4.	metoda projektów

NARZĘDZIA DYDAKTYCZNE

1.	platforma e-learningowa
2.	prezentacja multimedialna
	biblioteki cyfrowe i zasoby online

OPROGRAMOWANIE

1.	MS Powerpoint

OBCIĄŻENIE STUDENTA PRACĄ

	Forma aktywności	**Liczba godzin na zrealizowanie aktywności**	
		tryb stacjonarny	*tryb niestacjonarny*
1.	godziny kontaktowe z nauczycielem akademickim	**30**	**24**
2.	samodzielne przygotowanie do zajęć	20	20
3.	przygotowanie do kolokwium, egzaminu i innych form	25	25
4.	udział w konsultacjach	2	2
5.	zapoznanie się z literaturą przedmiotu	22	28
6.	egzamin	1	1
	SUMA GODZIN	**100**	**100**
	LICZBA PUNKTÓW ECTS	**4**	**4**

LITERATURA PODSTAWOWA

1.	Muliński, T., Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji, Warszawa 2015
2.	Kosiński J., Paradygmaty cyberprzestępczości, Warszawa 2015

LITERATURA UZUPEŁNIAJĄCA I ŹRÓDŁA PRAWA

1.	https://edu.pjwstk.edu.pl/wyklady/bsi/scb/index91.html
2.	https://edu.pjwstk.edu.pl/wyklady/bsi/scb/index99.html
3.	https://www.centrumxp.pl/Publikacja/Microsoft-liderem-analityki-bezpieczenstwa-wedlug-Forrester-Wave
4.	Korusiewicz, A., Zagrożenia w sieci Internet, Warszawa 2007
5.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560)

INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE:	
1.	PLATFORMA MOODLE zawiera: ▪ materiały dydaktyczne do przedmiotu ▪ przedmiotowe efekty uczenia się ▪ zalecaną literaturę ▪ warunki i kryteria zaliczenia przedmiotu
2.	BIBLIOTEKA WSZOP zapewnia literaturę podstawową do przedmiotu oraz wybrane pozycje literatury uzupełniającej, w tym dostęp do zbiorów cyfrowych i Platformy IBUK Libra
3.	ELEKTRONICZNY NIEZBĘDNIK STUDENTA zawiera: ▪ kierunkowe efekty uczenia się ▪ karty przedmiotów ▪ terminy konsultacji nauczycieli akademickich
4.	WIRTUALNY DZIEKANAT zawiera: ▪ harmonogram zajęć na bieżący semestr ▪ harmonogram sesji egzaminacyjnej ▪ ogłoszenia dotyczące organizacji roku akademickiego
5.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny jakościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ w pełni – ocena bardzo dobry ▪ z niewielkimi niedociągnięciami – ocena dobry plus ▪ z brakami, które można uzupełnić – ocena dobry ▪ z istotnymi brakami, które można uzupełnić – ocena dostateczny plus ▪ z istotnymi brakami na minimalnym poziomie – ocena dostateczny lub ▪ nie zostały osiągnięte – ocena niedostateczny.
6.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny ilościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ 91-100% sumy – ocena bardzo dobry ▪ 81-90% – ocena dobry plus ▪ 71-80% – ocena dobry ▪ 61-70% – ocena dostateczny plus ▪ 51-60% – ocena dostateczny lub ▪ 50% i mniej – ocena niedostateczny.
7.	Terminy egzaminów uzgadnia starosta roku z prowadzącym zajęcia
8.	Karta przedmiotu obowiązuje od roku akademickiego 2024/25