KARTA PRZEDMIOTU

I. OGÓLNE INFORMACJE O PRZEDMIOCIE								
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Bezpieczeństwo Wewnętrzne						
Specjalność:								
Profil studiów:		Praktyczny						
Forma studiów:		Stacjonarne i niestacjonarne						
Nazwa przedmiotu:		**Bezpieczeństwo w cyberprzestrzeni**						
Język wykładowy:		Język polski						
Kod przedmiotu kształcenia:		BW1K12						
Poziom studiów ***(I lub II stopień)***	I stopień	**Formy prowadzenia zajęć i liczba godzin w planie studiów:**						
Rok studiów:	2							
Semestr:	4	Wykład	Ćwiczenia	Seminarium	Laboratorium	Warsztaty	Zajęcia praktyczne	Praktyka zawodowa
Liczba punktów ECTS:	1	20/12				10/6		
Forma zaliczenia:		Zaliczenie na ocenę						
Wymagania wstępne w zakresie wiedzy oraz umiejętności:		Znajomość konstytucyjnych organów państwa odpowiedzialnych za bezpieczeństwo wewnętrzne. Znajomość instytucji państwowych odpowiedzialnych za zapewnienie porządku publicznego. Znajomość sieci oraz komunikacji interpersonalnej w internecie.						

II. CELE KSZTAŁCENIA

Cele kształcenia:

Cel 1: Nabycie podstawowej wiedzy w zakresie funkcjonowania sieci oraz zagrożeń wynikających z funkcjonowaniem stosunków międzyludzkich w zakresie cyberprzestrzeni..
Cel 2: Pozyskanie niezbędnej wiedzy w zakresie rozpoznawania zagrożeń w obrębie cyberprzestrzeni, które mają bezpośredni wpływ na bezpieczeństwo: światowe, państwowe, korporacyjne, ludzkie, itd.
Cel 3: Pozyskanie niezbędnej wiedzy dotyczącej rozpoznawania przestępczości zorganizowanej oraz penalizacji cyberprzestępstw.

III. PRZEDMIOTOWE EFEKTY KSZTAŁCENIA WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW

Efekt	Student, który zaliczył przedmiot w zakresie:	Odniesienie do kierunkowych efektów kształcenia	Metody weryfikacji
	wiedzy:		
W-1	Student rozumie i dostrzega zagrożenia w obszarze bezpieczeństwa państwa polskiego i bezpieczeństwa europejskiego, w tym rozumie zasady współpracy międzynarodowej w zakresie bezpieczeństwa w okresie pokoju i wojny.	K_W09	odpowiedź pisemna (kolokwium) na podstawie analizy literatury przedmiotu, esej na wybrane tematy dotyczące bezpieczeństwa cyberprzestrzeni
W-2	Student identyfikuje i analizuje symptomy przestępczości kryminalnej, gospodarczej i zorganizowanej oraz rozumie mechanizmy zwalczania tej przestępczości	K_W019	odpowiedź pisemna (kolokwium) na podstawie analizy literatury przedmiotu, esej na wybrane tematy dotyczące bezpieczeństwa cyberprzestrzeni

K_W3	Student definiuje, rozpoznaje i ocenia zagrożenia terrorystyczne w skali kraju i w skali międzynarodowej oraz ocenia sytuację kryzysową w przypadku ataku terrorystycznego		odpowiedź pisemna (kolokwium) na podstawie analizy literatury przedmiotu, esej na wybrane tematy dotyczące bezpieczeństwa cyberprzestrzeni
U-1	Student analizuje i ocenia stan bezpieczeństwa państwa polskiego i bezpieczeństwa europejskiego.	K_U08	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach ćwiczeń
U-2	Student przewiduje zagrożenia bezpieczeństwa społeczności lokalnych oraz zapobiega im stosując dostępne środki i metody, w tym uczestniczy przy zmienianiu kryminogennych aspektów przestrzeni	K_U12	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach ćwiczeń
U-3	Student przygotowuje prace pisemne, wystąpienia ustne oraz komunikuje się z otoczeniem	K_U20	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach ćwiczeń
K-1	Student rozumie potrzebę uczenia się przez całe życie	K_K01	ocena realizacji zadań przygotowanych w ramach ćwiczeń, ocena zaangażowania w pracę grupy, ocena zachowań i aktywności w trakcie wykładów i ćwiczeń, ocena prowadzenia merytorycznej dyskusji

IV. TREŚCI KSZTAŁCENIA

Treści kształcenia (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)

Wykład:		
Kod	Tematyka zajęć	Liczba godzin
W1 W2	Podstawowe zagadnienia dotyczące cyberprzestrzeni, cyberprzestępczości – definicje, miejsce w naukach społecznych, prawnych, ścisłych, itd.	4/1,5
W3 W4	Problematyka bezpieczeństwa informacji, jako istotnego czynnika bezpieczeństwa narodowego. Prawne aspekty bezpieczeństwa informacji niejawnych i innych chronionych z mocy prawa.	4/1,5
W5 W6	Charakterystyka przestępczości w obrębie cyberprzetrzeni: złośliwe oprogramowanie(malware), spam: nigeryjski, fałszywa reklama, portale społecznościowe, kradzież tożsamości, botnet.	4/1,5
W7 W8	Phishing. Ddos. Darknet: TOR, I2P, Freenet.	4/1,5
W9 W10	Płatności internetowe, kryptowaluty. Pranie pieniędzy. Carding. Internet ipr.	4/1,5
W11 W12	Pornografia dziecięca i pedofilia. Hazard internetowy. Oszustwa na aukcjach internetowych. Oszustwa telekomunikacyjne.	4/1,5
W13 W14	Zwalczanie cyberprzestępczości. Cyberprzestępczość a przestępczość zorganizowana.	4/1,5
W15	Współczesne zagrożenia w obrębie cyberprzestrzeni (zagrożenia asymetryczne, wojna hybrydowa).	4/1,5

Warsztaty:		
Kod	Tematyka zajęć	Liczba godzin
WT1	Omówienie wojny hybrydowej – praca zespołowa.	1
WT2	Omówienie zagrożeń asymetrycznych – praca zespołowa.	1
WT3	Phishing – zagadnienia praktyczne.	1
WT4	Ddos, malware, spam nigeryjski.	1
WT5	Płatności internetowe, kryptowaluty. Pranie pieniędzy – studium przypadków.	2
WT6	Pornografia dziecięca i pedofilia – geneza zagrożeń, postepowanie sprawców.	1
WT7	Darknet: TOR, I2P, Freenet.	3

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: wykład informacyjny (konwencjonalny),wykład konwersatoryjny, pokaz, burza mózgów, ćwiczenia praktyczne, ćwiczeniowa oparta na wykorzystaniu różnych źródeł wiedzy,dyskusja, analiza literatury przedmiotu, metoda projektów.

2. Narzędzia (środki) dydaktyczne: prezentacje multimedialne, podręczniki, wzory dokumentów, Internet, rzutniki multimedialne.

VI. FORMA I KRYTERIA ZALICZENIA PRZEDMIOTU

Forma zaliczenia przedmiotu. Kryteria oceny formującej:

1. Kolokwium – kryteria oceny:
    1. 51% - 60% - ocena dostateczna,
    2. 61% - 70% - ocena dostateczna plus,
    3. 71% - 80% - ocena dobra,
    4. 81% - 90% - ocena dobra plus,
    5. 91% - 100% - ocena bardzo dobra.

2. Przygotowanie eseju – kryteria oceny:
    1. **3,0 (dostateczny)** – przygotowanie i prezentacja na forum prezentacji,
    2. **3,5 (dostateczny plus)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej,
    3. **4,0 (dobry)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych,
    4. **4,5 (dobry plus)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania,
    5. **5,0 (bardzo dobry)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania, pomysłowość proponowanych rozwiązań.

Wymagania formalne:

1/ objętość eseju - max. 2 strony znormalizowanego
maszynopisu, tzn. marginesy 2,5 cm, odstęp 1,5; czcionka 12; TnT N;
2/ w tytule pliku własne imię i nazwisko oraz tytuł eseju.
3)Tematy do wyboru:

1. Omów zagadnienie bezpieczeństwa zewnętrznego oraz wewnętrznego w kontekście zapewnienia bezpieczeństwa w cyberprzestrzeni.
2. Omów instytucje odpowiedzialne za zapewnienie bezpieczeństwa w cyberprzestrzeni.
3. Czy Polska jest przygotowana na zagrożenia w cyberprzestrzeni – na podstawie konkretnych przykładów uzasadnij tak/nie?
4. Omów przestępstwa w obrębie cyberprzestrzeni.
5. Omów zagrożenia cyberprzestrzeni ze strony organizacji terrorystycznych.
6. Omów zagrożenia nieletnich wynikające z korzystania z komputerów.
7. Omów zagrożenia nieletnich wynikające z korzystania z internetu.
8. Czy Twoim zdaniem Policja lub inne organy państwa skutecznie zwalczają patologie i zagrożenia w obrębie użytkowników internetu? Tak/nie uzasadnij.
9. Czy społeczeństwo polskie jest przygotowane na zagrożenia wynikające z cyberprzestrzeni?
10. Czy potrafimy sami wpływać na własne bezpieczeństwo w cyberprzestrzeni?
11. Czy państwo może być cenzorem internetu? Jak Twoim zdaniem powinniśmy kreować zagadnienia bezpieczeństwa w obrębie cyberprzestrzeni?
12. Omów zagrożenia w cyberprzestrzeni dotyczące bezpieczeństwa państwa.
13. Omów zagrożenia w cyberprzestrzeni dotyczące bezpieczeństwa instytucji.
14. Omów zagrożenia w cyberprzestrzeni dotyczące bezpieczeństwa osób.
15. Czy portale społecznościowe są przydatne, czy też stanowią platformę do zdobycia informacji o przyszłych ofiarach- uzasadnij.

3. Obserwacja i ocena postaw studenta wynikających z:
    1. realizacji zadań przygotowanych w ramach ćwiczeń,
    2. zaangażowania w pracę grupy,
    3. zachowań i aktywności w trakcie wykładów i ćwiczeń,
    4. prowadzenia merytorycznej dyskusji,
    5. potrzeby ciągłego rozwoju osobistego i zawodowego.

Kryteria oceny podsumowującej:

6. średnia ocen formujących

Koordynator przedmiotu:	mgr Edward Polakiewicz

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	
Udział w wykładach	20/12
Udział w warsztatach	10/6
Udział w kolokwium zaliczeniowym	2/2

Samodzielna praca studenta (godziny niekontaktowe)	
Przygotowanie do warsztatów	5/5
Przygotowanie do kolokwium zaliczeniowego	3/5
Kwerenda internetowa	0/10
Opracowanie eseju	
Inne (jakie?) Przygotowanie materiałów do prezentacji multimeseju, analiza literatury przedmiotu	5/5
Łączna liczba godzin	**45/45**
Punkty ECTS za przedmiot	**1**

VIII. LITERATURA PRZEDMIOTU

Literatura podstawowa:
J. Kosiński – Paradygmaty cyberprzestępczości; wyd. I, wyd. Difin SA, Warszawa 2015,
K. Linderman – Bezpieczeństwo informacyjne. Nowe wyzwania; wyd. II, wyd. PWN SA, Warszawa 2017

Literatura uzupełniająca:
Praca zbiorowa pod red. J. Kosińskiego – Przestępczość teleinformatyczna; Wyd. WSPol Szczytno 2009

Praca zbiorowa pod red. M. Tanasia i S. Galanciak – Cyberprzestrzeń człowiek edukacja. Cyfrowa przestrzeń kształcenia; wyd. Of. Wyd. „Impuls", Kraków 2015