KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY **WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH**								
Kierunek studiów:		**Bezpieczeństwo wewnętrzne**						
Poziom studiów:		Drugiego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne						
Nazwa modułu:		**Bezpieczeństwo w cyberprzestrzeni w ujęciu indywidualnym oraz instytucjonalnym**						
Rodzaj modułu:		obowiązkowy						
Język wykładowy:		Język polski						
Rok studiów:	1	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	2	Wykład	Ćwiczenia	Seminarium	Praktyka zawodowa	Warsztaty	***	***
Liczba punktów ECTS ogółem:	4	20	-	-	-	46	-	-
Forma zaliczenia:		Egzamin						
Wymagania wstępne:		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 globalnych oraz lokalnych sieci oraz zagrożeń wynikających z funkcjonowaniem stosunków międzyludzkich w cyberprzestrzeni.

Cel 2: Pozyskanie niezbędnej wiedzy w zakresie rozpoznawania zagrożeń w obrębie cyberprzestrzeni, które mają bezpośredni wpływ na bezpieczeństwo: światowe, państwowe, korporacyjne, ludzkie, tworzenia polityk bezpieczeństwa z uwzględnieniem specyfiki systemu informatycznego.

Cel 3: Pozyskanie niezbędnej wiedzy dotyczącej rozpoznawania przestępczości zorganizowanej, penalizacji cyberprzestępstw, efektywnej współpracy z organami powołanymi do zapewnienia bezpiepieczeństwa i zwalczania przestępczości w cyberprzestrzeni.

III. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW

Efekt	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych	Metody weryfikacji
wiedzy:			
W01	zna i rozumie w pogłębionym stopniu - znaczenie nauk o bezpieczeństwie i komplementarnych wobec nich nauk prawnych, nauk o zarządzaniu i jakości oraz nauk o polityce i administracji, historii w funkcjonowaniu państwa, w tym uwarunkowania instytucjonalne, systemowe, polityczne, prawne systemu bezpieczeństwa wewnętrznego i zewnętrznego oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej.	K2BW_W02	Ustny lub pisemny sprawdzian wiedzy
W02	zna i rozumie w pogłębionym stopniu - systemy, procesy, uwarunkowania działalności w zakresie bezpieczeństwa społecznego, politycznego, ekonomicznego, gospodarczego, narodowościowego oraz struktury i instytucje odpowiedzialne za jego zagwarantowanie a także zastosowanie praktyczne tej wiedzy w działalności zawodowej.	K2BW_W04	
W03	zna i rozumie w pogłębionym stopniu - rodzaje i źródła zagrożeń	K2BW_W05	

	.bezpieczeństwa i procesy warunkujące pojawienie się, narastanie, rozprzestrzeniane, rozpoznanie i eliminację rzeczywistych i potencjalnych zagrożeń oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej.		
W04	Zna i rozumie w pogłębionym stopniu - organizację, funkcjonowanie i uwarunkowania działalności państwa w obszarze budowania i utrzymania bezpieczeństwa ochronnego i obronnego oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej.	K2BW_W07	
umiejętności:			
U01	Potrafi wykorzystać posiadaną wiedzę teoretyczną do szczegółowego opisu i praktycznego analizowania przyczyn i przebiegu procesów i zjawisk w obszarze nauk o bezpieczeństwie, nauk prawnych, nauk o zarządzaniu i jakości, nauk o polityce i administracji, historii, a także potrafi formułować własne opinie.	K2BW_U01	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów
U02	Potrafi wykorzystywać zasady, sposoby oraz techniczne metody i środki rozpoznawania, a także wykrywania prawnie określonych, ujemnych zjawisk społecznych oraz udowadniania istnienia lub braku związku między osobami a zdarzeniami, także zastosować praktyczne umiejętności w działalności zawodowej.	K2BW_U14	
U03	Potrafi wykorzystywać umiejętności, techniki, metody, systemy do wykrywania i zapobiegania przestępstwom oraz do organizacji bezpiecznej imprezy masowej i zgromadzeń publicznych, posługiwania się bronią a także zastosować praktyczne umiejętności w działalności zawodowej.	K2BW_U15	
kompetencji społecznych:			
K01	jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści.	K2BW_K01	ocena realizacji zadań, zaangażowania w pracę grupy, zachowań i aktywności, prowadzenia merytorycznej dyskusji

IV. TREŚCI PROGRAMOWE

Wykład

Kod	Tematyka zajęć	Liczba godzin
W1	Cyberprzestrzeń – definicja, cechy, zasadnicze elementy, definicja według polskiego prawa, rola definicji cyberprzestrzeni w obszarze bezpieczeństwa państwa, materiały Ministerstwa Cyfryzacji na temat cyberprzestrzeni.	4
W2	Ministerstwo Cyfryzacji - podstawy prawne, wizja, misja, wartości, zadania, współpraca międzynarodowa, Departament Cyberbezpieczeństwa, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na latach 2019-2024, cele szczegółowe Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na latach 2019-2024.	4
W3	Ustawa o krajowym systemie cyberbezpieczeństwa, określenie incydentu w cyberprzestrzeni ilość i podział incydentów, jednostki reagujące na incydenty w systemach informatycznych, Program Współpracy w Cyberbezpieczeństwie (PWCyber).	2
W4	Rządowe Programy Ochrony Cyberprzestrzeni, definicje przestępczości informatycznej według Interpolu, Rady Europy, Unii Europejskiej, ONZ, rodzaje przestępstw związanych z użytkowaniem systemów informatycznych, ich cechy, przestępstwa charakterystyczne dla cyberprzestępczości, penalizacja przestępstw informatycznych, zagrożenia asymetryczne, pornografia dziecięca w ujęciu Konwencji RE – art. 9 .	4
W5	Prawo do bycia zapomnianym w Internecie, geneza, Rozporządzenie unijnego RODO (art. 17 ust. 1), warunki usunięcia danych, wyjątki od konieczności egzekwowania przez Administratora prawa do bycia zapomnianym.	4
W6	Kopie i archiwa stron internetowych, „Maszyna czasu” – cele, dowody sądowe z archiwów stron internetowych.	2

Warsztaty

Kod	Tematyka zajęć	Liczba godzin
Wt1	Zapewnienie autentyczności i integralności zapisów cyfrowych, funkcja skrótu, praktyczne wykorzystanie oprogramowania haszującego .	8
Wt2	Podstawowe pojęcia dotyczące sieci komputerowych, budowa i złożoność Internetu, budowa sieci lokalnych, przykładowe pojęcia słowniczka cyberbezpieczeństwa, zagrożenia i przestępstwa, reagowanie na przemoc seksualną względem dziecka w sieci, gdzie zgłaszać i jak się zachować, omówienie przypadków, ogólne zasady bezpieczeństwa i higieny cyfrowej,	8

	bezpieczne hasła, programy peer-to-peer (P2P).	
Wt3	Instytucje powołane do zapewnienia cyberbezpieczeństwa, zwalczania cyberprzestepczości, struktura, zadania, kanały komunikacji.	8
Wt4	Polityka bezpieczeństwa – definicja, etapy tworzenia, zarządzanie, monitorowanie i konserwacja, zakres, akty prawne obowiązujące w Polsce związane z polityką bezpieczeństwa, omówienie przykładowej Polityki Bezpieczeństwa.	10
Wt5	Pozyskiwanie danych - biały wywiad, czym jest, czego szukamy, słowa kluczowe, parametry, operatory.	6
Wt6	Bezpieczeństwo osobiste w cyberprzestrzeni, omówienie i konfigurowanie parametrów prywatności, rodzaje i podział zagrożeń, socjotechnika w cyberprzestrzeni, fałszywe poczucie bezpieczeństwa, analiza przykładów zidentyfikowanych incydentów w systemach informatycznych.	6

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: wykład informacyjny, warsztaty oparte na wykorzystaniu różnych źródeł wiedzy, dyskusja.

2. Narzędzia (środki) dydaktyczne: wykład informacyjny, warsztaty oparte na wykorzystaniu różnych źródeł wiedzy, dyskusja.

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

Forma zaliczenia modułu.

Kryteria oceny formującej:

1. Ustny lub pisemny sprawdzian wiedzy – kryteria oceny:
   - 51% - 60% - ocena dostateczna,
   - 61% - 70% - ocena dostateczna plus,
   - 71% - 80% - ocena dobra,
   - 81% - 90% - ocena dobra plus,
   - 91% - 100% - ocena bardzo dobra.
2. Przygotowanie prezentacji oraz praca badawcza – kryteria oceny:
   - 3,0 (dostateczny) – przygotowanie i prezentacja na forum prezentacji,
   - 3,5 (dostateczny plus) – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej,
   - 4,0 (dobry) – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy
   - i syntezy treści źródłowych,
   - 4,5 (dobry plus) – przygotowanie prezentacji i ich prezentacja na forum, elementy pracy badawczej oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania,
   - 5,0 (bardzo dobry) – przygotowanie prezentacji i ich prezentacja na forum, elementy pracy badawczej oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania, pomysłowość proponowanych rozwiązań.
3. Obserwacja i ocena postaw studenta wynikających z:
   - realizacji zadań przygotowanych w ramach ćwiczeń,
   - zaangażowania w pracę grupy,
   - zachowań i aktywności w trakcie wykładów i ćwiczeń,
   - prowadzenia merytorycznej dyskusji,
   - potrzeby ciągłego rozwoju osobistego i zawodowego.

Kryteria oceny podsumowującej:

- średnia ocen formujących z poszczególnych form zaliczenia

Ocena podsumowująca:

- średnia ocen z wykładów i warsztatów

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**66**
Udział w wykładach	20
Udział w innych formach zajęć -warsztaty	46
Samodzielna praca studenta (godziny niekontaktowe)	**34**
Przygotowanie do wykładu	12
Przygotowanie do innych form zajęć -warsztaty	12

Przygotowanie do egzaminu	6
Przygotowanie do zaliczenia	4
Kwerenda internetowa	24
Łączna liczba godzin	**100**
Punkty ECTS za moduł	**4**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. J. Kosiński – Paradygmaty cyberprzestępczości; wyd. Difin SA, Warszawa 2015,
2. K. Linderman – Bezpieczeństwo informacyjne. Nowe wyzwania; wyd. PWN SA, Warszawa 2017
3. P. Dela - Teoria walki w cyberprzestrzeni; Akademia Sztuki Wojennej, Warszawa 2020

Literatura uzupełniająca:

1. Praca zbiorowa pod red. J. Kosińskiego – Przestępczość teleinformatyczna; Wyd. WSPol Szczytno 2015
2. T. Trejderowski – Kradzież tożsamości: terroryzm informatyczny: cyberprzestępstwa, internet, telefon, Facebook; wyd. Eneteia Wydawnictwo Psychologii i Kultury, Warszawa 2013