KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY Wydział Nauk Społecznych i Humanistycznych								
Kierunek studiów:		Kierunek Bezpieczeństwo wewnętrzne						
Poziom studiów:		pierwszego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne/niestacjonarne						
Nazwa modułu:		**Bezpieczeństwo w cyberprzestrzeni**						
Rodzaj modułu:		Obowiązkowy						
Język wykładowy:		Język polski						
Rok studiów:	2	Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:						
Semestr:	4	Wykład	Warsztaty	**	**	**	**	**
Liczba punktów ECTS ogółem:	3	16	18	S/N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Zaliczenie na ocenę						
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 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. 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 uwarunkowania (w tym m.in.: społeczne, instytucjonalne, funkcjonalne, prawne, gospodarcze, polityczne i administracyjne) występujące w otoczeniu wewnętrznym i zewnętrznym systemu bezpieczeństwa w skali międzynarodowej, państwowej, regionalnej i lokalnej .	K1BW_W04	Ustny lub pisemny sprawdzian wiedzy
W02	zna i rozumie wybrane zagadnienia szczegółowe z zakresu nauk o bezpieczeństwie .	K1BW_W06	
umiejętności:			
U01	potrafi wykonywać zadania typowe dla działalności zawodowej związanej z kierunkiem studiów, w tym np. związane z umiejętnością obrony w sytuacji zagrożenia .	K1BW_U02	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, realizacji zadań
U02	potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania problemów z obszaru bezpieczeństwa .	K1BW_U07	
kompetencji społecznych:			
K01	jest gotów do zasięgania opinii ekspertów w przypadku problemów z	K1BW_K02	ocena realizacji

	samodzielnym rozwiązaniem problemu i uwzględnienia otrzymanych informacji w dalszym postępowaniu .		zadań, zaangażowania w pracę grupy, zachowań i aktywności, prowadzenia merytorycznej dyskusji
K02	jest gotów do wypełniania zobowiązań społecznych, w tym inicjowania i współorganizowania działalności na rzecz środowiska społecznego i interesu publicznego .	K1BW_K03	

IV. TREŚCI PROGRAMOWE

**

Kod	Tematyka zajęć	Liczba godzin S/N
W1	- definicja cybeprzestrzeni - cechy cyberprzestrzeni (omówienie) - różne ujęcia cyberprzestrzeni (w zależności od dziedziny nauki) - zasadnicze elementy cybeprzestrzeni - różnice w podejściu do definiowania cyberprzestrzeni w różnych krajach i instytucjach - definicja cyberprzestrzeni według polskiego prawa - rola definicji cyberprzestrzeni w obszarze bezpieczeństwa państwa - materiały Ministerstwa Cyfryzacji na temat cyberprzestrzeni	4
W2	- Cyfryzacja KPRM podstawy prawne - Cyfryzacja KPRM - Wizja, misja, wartości, zadania - Cyfryzacja KPRM - współpraca międzynarodowa - Krajowy system cyberbezpieczeństwa - Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 - ustawa o krajowym systemie cyberbezpieczeństwa - definicje określane przez Ustawa Krajowy System Cyberbezpieczeństwa - jednostki, reagujące na incydenty w cyberprzestrzeni - określenie incydentu w cyberprzestrzeni - ilość i podział incydentów; - działania mające na celu wzmocnienie bezpieczeństwa użytkowników usług internetowych	4
W3	- Definicje cyberprzestępczości według Interpolu, Rady Europy, Unii Europejskiej, ONZ - Rodzaje cyberprzestępstw - Przestępstwa charakterystyczne dla cyberprzestępczości - Przestępstwa popełniane z wykorzystaniem sieci Internet - Najważniejsze cechy cyberprzestępczości - Zagrożenia asymetryczne - Penalizacja cyberprzestępstw - Penalizacja cyberprzestępstw – treści pornograficzne w tym z udziałem małoletnich - Pornografia dziecięca w ujęciu Konwencji RE – art. 9 - Nawoływanie do nienawiści na tle rasowym i treści ksenofobiczne, obrażanie uczuć religijnych - Groźby karalne, zmuszanie do określonego zachowania, cyberstalking, kradzież tożsamości i inne przestępstwa - Regulacje prawne ujęte w kodeksie wykroczeń	4
W4	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 - Kopie stron internetowych - procedura usuwania danych z kopii stron z serwisu Google - archiwa stron internetowych - „Maszyna czasu” – cele - dowody sądowe z archiwów stron internetowych	4

**

Kod	Tematyka zajęć	Liczba godzin S/N
	- podstawowe pojęcia dotyczące sieci komputerowych - budowa sieci lokalnych - budowa i złożoność Internetu - przykładowe pojęcia słowniczka cyberbezpieczeństwa – zagrożenia i przestępstwa	

WT1	- przykładowe pojęcia słowniczka cyberbezpieczeństwa – stan zagrożenia - jak reagować na przemoc seksualną względem dziecka w sieci – gdzie zgłaszać i jak się zachować - jak reagować na przemoc seksualną względem dziecka w sieci – omówienie przypadków - czym jest chmura i czy można mieć do niej zaufanie? - ogólne zasady bezpieczeństwai higieny cyfrowej – komputer, tablet, telefon, router sieci Wi-Fi, postępowanie własne - bezpieczne hasła – podstawowe zasady, blokady urządzeń, klawiatury wirtualne - programy peer-to-peer (P2P)	4
WT2	Biały wywiad - czym jest biały wywiad - czego wyszukujemy w internecie - istotne elementy białego wywiadu internetowego - słowa kluczowe - znaczenie parametrów wyszukiwania - jak tworzyć słowa kluczowe - najważniejsze pytania przy definiowaniu zagadnienia do opracowania - wykorzystanie operatorów logicznych - operatory inne - szukanie zaawansowane - możliwości serwisu Google - przykładowe ćwiczenia do pracy własnej	4
WT3	- Zwalczanie cyberprzestepczości przez Policję - Struktura Centralnego Biura Zwalczania Cyberprzestępczości - zadania Centralne Biuro Zwalczania Cyberprzestępczości - Zwalczanie cyberprzestępczości przez funkcjonariuszy Centralnego Laboratorium Kryminalistycznego Policji oraz Laboratoriów Kryminalistycznych Komend Wojewódzkich - Zadania pracowni do badań informatycznych Laboratoriów Kryminalistycznych Komend Wojewódzkich Policji	6
WT4	- Polityka bezpieczeństwa systemu IT - Zasady budowania Polityki bezpieczeństwa systemów IT - Definiowanie zasobów do ochrony - Mechanizmy wykorzystywane do budowy systemu bezpieczeństwa - Weryfikacja wykorzystanie Polityki bezpieczeństwa systemów IT	4

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 – 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 i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania,
   - 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.
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
- 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)	30
Udział w wykładach	14
Udział w innych formach zajęć (warsztaty)	16
Inne (jakie?)	
Samodzielna praca studenta (godziny niekontaktowe)	45
Przygotowanie do wykładu	20
Przygotowanie do innych form zajęć (warsztaty)	20
Przygotowanie do egzaminu	
Przygotowanie do zaliczenia innych zajęć (**)	
Inne (np. gromadzenie materiałów do projektu, kwerenda internetowa, opracowanie prezentacji multimedialnej itp.)	5
Łączna liczba godzin	75
Punkty ECTS za moduł	3

VIII. ZALECANA LITERATURA

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

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