KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:	Bezpieczeństwo wewnętrzne							
Poziom studiów:	Pierwszego stopnia							
Profil studiów:	praktyczny							
Forma studiów:	stacjonarne							
Nazwa modułu:	**Nowoczesne technologie bezpieczeństwa osobistego i instytucjonalnego**							
Rodzaj modułu:	obowiązkowy							
Język wykładowy:	Język polski							
Rok studiów: II	Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:							
Semestr: IV	Wykład	Warsztaty	**	**	**	**	**	
Liczba punktów ECTS ogółem: 3	10	20	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 wiedzy w zakresie poruszania się w cyberprzestrzeni w aspekcie zagrożeń indywidualnych jak i militarnych i terrorystycznych. **Cel 2:** Pozyskanie niezbędnej wiedzy w zakresie działania osobistych sieci komputerowych, korzystania z social mediów, bankowości internetowej. **Cel 3**: Pozyskanie niezbędnej wiedzy dotyczącej procedur postępowania przy wstępowaniu incydentów w cyberprzestrzeni, systemów bezpieczeństwa informatycznego, polityk bezpieczeństwa organizacji, firm, przedsiębiorstw itp.

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 - charakter nauk społecznych i ich relacje do innych nauk	K1BW_W01	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów
W02	zna i rozumie w zaawansowanym stopniu - wybrane fakty, obiekty i zjawiska z zakresu nauk społecznych ze szczególnym uwzględnieniem nauk o bezpieczeństwie oraz nauk o polityce i administracji, nauk o zarządzaniu i jakości, nauk prawnych i socjologicznych.	K1BW_W02	
W08	zna i rozumie w pogłębionym stopniu - możliwości praktycznego zastosowania zdobytej interdyscyplinarnej wiedzy związanej z bezpieczeństwem, a także właściwej dla zakresu badawczego nauk o polityce i administracji, nauk o zarządzaniu i jakości, nauk prawnych i socjologicznych, również w trakcie prowadzenia działalności zawodowej i podczas praktyk zawodowych .	K1BW_W08	
umiejętności:			
U01	potrafi wykorzystać posiadaną wiedzę teoretyczną poprzez praktyczne wykorzystanie posiadanej wiedzy w formułowanie i rozwiązywanie złożonych i nietypowych problemów z zakresu bezpieczeństwa .	K1BW_U01	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia
U02	potrafi właściwie dobierać źródła i pochodzące z nich informacje przy analizie i prognozowaniu potencjalnych i rzeczywistych zagrożeń bezpieczeństwa (w tym m.in. prawnych, politycznych, kulturowych, społecznych i ekonomicznych) w aspekcie międzynarodowym,	K1BW_U03	

	państwowym, regionalnym i lokalnym .		merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów
U03	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 samodzielnym rozwiązaniem problemu i uwzględnienia otrzymanych informacji w dalszym postępowaniu .	K1BW_K02	ocena realizacji zadań, zaangażowania w pracę grupy, zachowań i aktywności, prowadzenia merytorycznej dyskusji
K02	jest gotów do myślenia i działania w sposób przedsiębiorczy .	K1BW_K04	

IV. TREŚCI PROGRAMOWE

Wykład

Kod	**Tematyka zajęć**	Liczba godzin S/N
W1	Cyberprzestrzeń jako nowe środowisko funkcjonowania społeczeństwa, zasadnicze elementy, rola w obszarze bezpieczeństwa państwa	2
W2	Podstawowe elementy lokalnych sieci komputerowych	2
W3	Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa jako cel szczegółowy Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024	2
W4	Incydenty w cyberprzestrzeni, procedury reagowania jako element polityki bezpieczeństwa organizacji	4

Warsztaty

Kod	Tematyka zajęć	Liczba godzin S/N
Wt1	Główne zagrożenia związane z wykorzystaniem cyberprzestrzeni	4
Wt2	Funkcjonalność cyberprzestrzeni na potrzeby e-społeczeństwa	4
Wt3	Bezpieczeństwo użytkownika social mediów i bankowości internetowej – analiza zabezpieczeń	4
Wt4	Podstawowe aspekty prawidłowego wykorzystania cyberprzestrzeni - zasady bezpieczeństwa i higieny cyfrowej	4
Wt5	Przykładowa polityka bezpieczeństwa – analiza przypadku	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

1. Sposób zaliczenia:
- ~~egzamin~~
- zaliczenie z oceną
- ~~zaliczenie bez oceny~~

2. Formy zaliczenia:
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.

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.

3. Podstawowe kryteria średnia ocen formujących z poszczególnych form zaliczenia, 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	10
Udział w innych formach zajęć (**)	20
Samodzielna praca studenta (godziny niekontaktowe)	45
Przygotowanie do wykładu	10
Przygotowanie do innych form zajęć (**)	20
Przygotowanie do egzaminu	
Przygotowanie do zaliczenia innych form zajęć (**)	15
Łączna liczba godzin	75
Punkty ECTS za moduł	3

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. M. Molendowska, R. Miernik - Bezpieczeństwo w cyberprzestrzeni : wybrane zagadnienia. Wydawnictwo Adam Marszałek 2020r.
2. J. Stelmach - Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej. T. 4. Wydawnictwo Delfin 2022r.
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