KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Bezpieczeństwo wewnętrzne						
Poziom studiów:		I stopień						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne						
Nazwa modułu:		**Bezpieczeństwo w cyberprzestrzeni**						
Rodzaj modułu:		obowiązkowy						
Język wykładowy:		Język polski						
Rok studiów:	II	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	IV	Wykłady	Warsztaty	**	**	**	**	**
Liczba punktów ECTS ogółem:	5	20	40	S/N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Egzamin						
Wymagania wstępne:		Ogólna znajomość pojęć z obszaru bezpieczeństwa wewnętrznego.						

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 oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej	K1BW_W04	Obserwacja zachowań, aktywność na zajęciach, egzamin
W02	Zna i rozumie wybrane zagadnienia szczegółowe z zakresu nauk o bezpieczeństwie oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej	K1BW_W06	Obserwacja zachowań, aktywność na zajęciach, egzamin
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	Obserwacja zachowań, aktywność na zajęciach, egzamin
U02	Potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania problemów z obszaru bezpieczeństwa a także zastosować praktyczne umiejętności w działalności zawodowej	K1BW_U07	Obserwacja zachowań, aktywność na zajęciach, egzamin

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	Obserwacja zachowań, aktywność na zajęciach, egzamin
K02	Jest gotów do wypełniania zobowiązań społecznych, w tym inicjowania i współorganizowania działalności na rzecz środowiska społecznego i interesu publicznego	K1BW_K03	Obserwacja zachowań, aktywność na zajęciach, egzamin

IV. TREŚCI PROGRAMOWE

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

WYKŁADY

Kod	Tematyka zajęć	Liczba godzin S/N
W1	Penalizacja przestępstw związanych z cyberprzestrzenią	4
W2	Ministerstwo cyfryzacji - Wizja, misja, wartości, zadania, współpraca międzynarodowa,	4
W3	Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, ustawa o krajowym systemie cyberbezpieczeństwa,	4
W4	Definicje cyberprzestępczości według Interpolu, Rady Europy, Unii Europejskiej, ONZ, Rodzaje, cechy, penalizacja cyberprzestępstw	4
W5	„Nie istnieje bezpieczeństwo absolutne” etapy i zasady tworzenia systemu bezpieczeństwa; bezpieczne hasła, kopie danych – tworzenie, zarządzania;	4

WARSZTATY

Kod	Tematyka zajęć	Liczba godzin S/N
WT1	Sieci komputerowe – podstawowe pojęcia, budowa, elementy, zalety i zagrożenia	6
WT2	Dezinformacja, fake news, stalking, trollowanie – zagrożenia; edukacja jako narzędzie przeciwdziałania	8
WT3	Incydenty w sieci – typy, efekty, podatności, analiza przykładów	8
WT4	Instytucje do zwalczania cyberprzestępczości CBZC, Laboratoria kryminalistyki, Prokuratura, NASK	6
WT5	Biały wywiad (OSINT), cele, narzędzia, zakres	6
WT6	Procedury bezpieczeństwa - przykłady	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

1. Sposób zaliczenia:

- egzamin

2. Formy zaliczenia:

1) Wykład – pisemny test wiedzy z pytaniami otwartym/zamkniętymi obejmujący swoim zakresem treści programowe zaprezentowane podczas wykładów:
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) Warsztaty - udział i wykonywanie prac praktycznych w trakcie zajęć oraz 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 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 warsztatów,
- zaangażowania w pracę grupy,
- zachowań i aktywności w trakcie wykładów i warsztatów,
- prowadzenia merytorycznej dyskusji,
- potrzeby ciągłego rozwoju osobistego i zawodowego.

3. Podstawowe kryteria: średnia ocen formujących z poszczególnych form zaliczenia

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**60**
Udział w wykładach	20
Udział w innych formach zajęć (**)	40
Samodzielna praca studenta (godziny niekontaktowe)	**65**
Przygotowanie do wykładu	20
Przygotowanie do innych form zajęć (**)	20
Przygotowanie do egzaminu	20
Przygotowanie do zaliczenia innych form zajęć (**)	5
Łączna liczba godzin	**125**
Punkty ECTS za moduł	**5**

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. Banasiński Cezary, Błaszczyk Cezary i inni, *Cyberbezpieczeństwo: zarys wykładu*; wyd. Wolters Kluwer Polska 2018
4. Krawiec Jerzy, *Cyberbezpieczeństwa: podejście systemowe;* wyd. Oficyna Wydawnicza Politechniki Warszawskiej 2019

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

*należy odpowiednio wypełnić

** należy wpisać formę/formy przypisane do modułu określone w programie studiów (ćwiczenia, seminarium, konwersatorium, lektorat, laboratorium, warsztat, projekt, zajęcia praktyczne, zajęcia terenowe, zajęcia wychowania fizycznego, praktyka zawodowa, inne)