KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Bezpieczeństwo wewnętrzne						
Poziom studiów:		Studia pierwszego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne						
Nazwa modułu:		**Bezpieczeństwo w cyberprzestrzeni**						
Rodzaj modułu:		moduły kształcenia kierunkowego						
Język wykładowy:		język polski						
Rok studiów:	II	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	4	Wykłady	Warsztaty	**	**	**	**	**
Liczba punktów ECTS ogółem:	5	20/12	40/24	S / N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Egzamin						
Wymagania wstępne:		Znajomość konstytucyjnych organów państwa odpowiedzialnych za bezpieczeństwo wewnętrzne. Znajomość instytucji państwowych odpowiedzialnych za zapewnienie porządku publicznego. Podstawowa znajomość sprzętu i oprogramowania systemowego, 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		
Efekt uczenia się	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych
wiedzy:		
W01	Zna i rozumie zalety i zagrożenia wynikające z wykorzystania cyberprzestrzeni w zakresie globalnym, krajowym i lokalnej oraz zastosować praktyczne tę wiedzę w zastosowaniu zawodowym lub domowym	K1BW_W04
W02	Zna i rozumie wybrane elementy systemów zabezpieczenia informatycznego od strony proceduralnej oraz zastosowanie praktyczne tej wiedzy w sferze zawodowej i prywatnej	K1BW_W06
umiejętności:		
U01	Potrafi zorganizować i nadzorować zlecone zadania dotyczące cyberbezpieczeństwa w sferze zawodowej, np. związane z wystąpieniem incydentu w systemach informatycznych	K2BW_U03
U02	Potrafi wykorzystywać zdobytą wiedzę z zakresu cyberbezpieczeństwa do tworzenia i przestrzegania zasad cyberbezpieczeństwa w sferze zawodowej i prywatnej	K2BW_U04
kompetencji społecznych:		
K01	Jest gotów do współdziałania z organami odpowiedzialnymi za cyberbezpieczeństwo oraz zasięgnąć ich rad w przypadku zagrożenia lub wystąpienia incydentu w systemach informatycznych oraz wdrożenie ich w	K1BW_K02

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	Zaznajomienie kartą modułu i formą zaliczenia . Penalizacja przestępstw związanych z cyberprzestrzenią	4/3
W2	Ministerstwo cyfryzacji - Wizja, misja, wartości, zadania, współpraca międzynarodowa,	4/3
W3	Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, ustawa o krajowym systemie cyberbezpieczeństwa,	4/2
W4	Definicje cyberprzestępczości według Interpolu, Rady Europy, Unii Europejskiej, ONZ, Rodzaje, cechy, penalizacja cyberprzestępstw	4/2
W5	„Nie istnieje bezpieczeństwo absolutne" etapy i zasady tworzenia systemu bezpieczeństwa; bezpieczne hasła, kopie danych – tworzenie, zarządzania;	4/2
Warsztaty		
Kod	Tematyka zajęć	Liczba godzin S/N
WT1	Sieci komputerowe – podstawowe pojęcia, budowa, elementy, zalety i zagrożenia	6/3
WT2	Dezinformacja, fake news, stalking, trollowanie – zagrożenia; edukacja jako narzędzie przeciwdziałania	8/5
WT3	Incydenty w sieci – typy, efekty, podatności, analiza przykładów	8/5
WT4	Instytucje do zwalczania cyberprzestępczości CBZC, Laboratoria kryminalistyki, Prokuratura, NASK	6/4
WT5	Biały wywiad (OSINT), cele, narzędzia, zakres	6/3
WT6	Procedury bezpieczeństwa - przykłady	6/4

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: wykład informacyjny, warsztaty oparte na wykorzystaniu różnych źródeł wiedzy, dyskusja.
2. Narzędzia (środki) dydaktyczne: prezentacje multimedialne, film, teksty źródłowe, dokumenty, Internet, rzutniki multimedialne

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

1. Formy zaliczenia:

- Wykłady - egzamin
- Warsztaty – zaliczenie z oceną prezentacji lub referatów obrazujących zlecone projekty

2. Sposób weryfikacji i oceniania efektów uczenia się:

wykłady: kolokwium – kryteria oceny:

- **3,0 (dostateczny)** – wypowiedzi niesamodzielne, odtwórcze, stereotypowe sądy, zakłócenia w kompozycji i spójności,
- **3,5 (dostateczny plus)** – powierzchowne odpowiedzi na pytania, dopuszczalne nieliczne błędy rzeczowe, spłycenie interpretacji tekstu,
- **4,0 (dobry)** – odpowiedzi na pytania z dopuszczalnymi niewielkimi błędami merytorycznymi, strukturalnymi i językowymi,
- **4,5 (dobry plus)** – odpowiedzi na pytania z dopuszczalnymi niewielkimi błędami strukturalnymi i językowymi
- **5,0 (bardzo dobry)** – pełna i bezbłędna odpowiedź na pytania z wykorzystaniem trzech kryteriów: kryterium merytorycznego, strukturalnego i językowego,

Warsztaty – rozwiązywanie zlecanych zadań /projektów

- 51% - 60% - ocena dostateczna,
- 61% - 70% - ocena dostateczna plus,
- 71% - 80% - ocena dobra,
- 81% - 90% - ocena dobra plus,
- 91% - 100% - ocena bardzo dobra.

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 oceny lub wymagania egzaminacyjne określane są indywidualnie, jednak powinny zachować adekwatność wobec zaplanowanych efektów uczenia się.

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**60/36**
Udział w wykładach	20/12
Udział w innych formach zajęć (warsztaty)	40/24
Samodzielna praca studenta (godziny niekontaktowe)	**65/ 89**
Przygotowanie do wykładu	25/34
Przygotowanie do innych form zajęć (warsztaty)	25/34
Przygotowanie do egzaminu	15/21
Przygotowanie do zaliczenia innych form zajęć (Warsztaty)	0
Łączna liczba godzin	**125**
Punkty ECTS za moduł	**5**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. K. Linderman*, Bezpieczeństwo informacyjne. Nowe wyzwania;* wyd. PWN SA, Warszawa 2017
2. Banasiński Cezary, Błaszczyk Cezary i inni, *Cyberbezpieczeństwo: zarys wykładu*; wyd. Wolters Kluwer Polska 2018
3. 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
3. J. Kosiński, *Paradygmaty cyberprzestępczości;* wyd. Difin SA, Warszawa 2015,