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:		**Wprowadzenie do cyberbezpieczeństwa**	
Rodzaj modułu:		obowiązkowy	
Język wykładowy:		Język polski	
Rok studiów:	II	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**	
Semestr:	III	Wykłady	Warsztaty
Liczba punktów ECTS ogółem:	4	20	24
Forma zaliczenia:		Zaliczenie na ocenę	
Wymagania wstępne:		Ogólna znajomość pojęć z obszaru bezpieczeństwa wewnętrznego.	

II. CELE KSZTAŁCENIA
Cele kształcenia:
Cel 1: przekazanie studentom wiedzy o podstawowych problemach cyberbezpieczeństwa w obszarach życia prywatnego i zawodowego. **Cel 2:** wykształcenie wśród studentów umiejętności właściwego reagowania na różnego rodzaju zagrożenia pojawiające się w sieci internetowej, umiejętności rozstrzygania dylematów związanych z administrowaniem oraz uzupełniania i doskonalenia nabytej wiedzy i umiejętności w warunkach postępu procesów cyfryzacji w administracji publicznej.

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 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
W02	Zna i rozumie wybrane zagadnienia szczegółowe z zakresu nauk o bezpieczeństwie oraz zastosowanie praktyczne tej wiedzy w działalności zawodowej	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
U02	Potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania problemów z obszaru bezpieczeństwa a także zastosować praktyczne umiejętności w działalności zawodowej	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
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
WYKŁADY

Kod	Tematyka zajęć	Liczba godzin
W1	Cybeprzestrzeń – definicje, cechy, elementy, rola definicji cyberprzestrzeni w obszarze bezpieczeństwa państwa	4
W2	Bezpieczeństwo w cyberprzestrzeni – dokumenty strategiczne	4
W3	Internet – powstanie i rozwój	4
W4	Praca i nauka zdalna – rekomendacje bezpieczeństwa	4
W5	Współpraca krajowa i międzynarodowa jako gwarancja cyberbezpieczeństwa	4
WARSZTATY		
Kod	Tematyka zajęć	Liczba godzin
WT1	Typy zagrożeń w cyberprzestrzeni, minimalizacja ryzyka	6
WT2	Sieci lokalne – elementy, wykorzystanie	6
WT3	Wymiana danych w sieci – narzędzia, zalety i zagrożenia	4
WT4	Przemoc w sieci – jak reagować, gdzie zgłaszać, co zabezpieczać, analiza przypadków	4
WT5	E-społeczeństwo – dostępne programy, narzędzia	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. Formy zaliczenia:

- zaliczenie z oceną

2. Sposób weryfikacji i oceniania efektów uczenia się:

1. Warsztaty - Przygotowanie prezentacji i/lub pisemny test wiedzy– kryteria oceny:

- **3,0 (dostateczny)** – przygotowanie i prezentacja na forum grupy,
- **3,5 (dostateczny plus)** – przygotowanie i prezentacja na forum grupy oraz znajomość literatury źródłowej,
- **4,0 (dobry)** – przygotowanie i prezentacja na forum grupy oraz znajomość literatury źródłowej, umiejętność analizy
  i syntezy treści źródłowych,
- **4,5 (dobry plus)** – przygotowanie i prezentacja na forum grupy oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania,
- **5,0 (bardzo dobry)** – przygotowanie i prezentacja na forum grupy oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania, pomysłowość proponowanych rozwiązań.

Test wiedzy:

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

2. 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 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)	**44**
Udział w wykładach	20
Udział w innych formach zajęć (warsztaty)	24
Samodzielna praca studenta (godziny niekontaktowe)	**56**
Przygotowanie do wykładu	22
Przygotowanie do innych form zajęć (warsztatów)	22
Przygotowanie do egzaminu	0
Przygotowanie do zaliczenia innych form zajęć (zaliczenia)	12
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. Banasiński Cezary, Błaszczyk Cezary i inni, *Cyberbezpieczeństwo: zarys wykładu*; wyd. Wolters Kluwer Polska 2018

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