KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Administracja						
Poziom studiów:		studia pierwszego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne						
Nazwa modułu:		**Wprowadzenie do cyberbezpieczeństwa**						
Rodzaj modułu:		moduł kształcenia podstawowego						
Język wykładowy:		Język polski						
Rok studiów:	1	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	2	Wykład	Warsztaty	**	**	**	**	**
Liczba punktów ECTS ogółem:	2	10	20	S/N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Zaliczenie z oceną						
Wymagania wstępne:		Wiedza i umiejętności z informatyki na poziomie szkoły średniej. Znajomość konstytucyjnych organów państwa odpowiedzialnych za bezpieczeństwo wewnętrzne. Znajomość instytucji państwowych odpowiedzialnych za zapewnienie porządku publicznego.						

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.

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 zasady bezpiecznego korzystania z zasobów cyberprzestrzeni	K1A_W13
W02	zna i rozumie zasady funkcjonowania instytucji odpowiedzialnych za cyberbezpieczeństwo w ujęciu europejskim, krajowym i lokalnym.	K1A_W15
umiejętności:		
U01	potrafi zidentyfikować zagrożenia i zaistniałe incydenty w cyberprzestrzeni oraz prawidłowo reagować	K1A_U17
kompetencji społecznych:		
K01	jest gotów na wspólne działania w zakresie poprawy cyberbezpieczeństwa w określonej organizacji realizując różne zadania, współdziałając z uprawnionymi organami	K1A_K03

IV. TREŚCI PROGRAMOWE		
Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)		
Wykład		
Kod	**Tematyka zajęć**	**Liczba godzin S**
W1	Zapoznanie z kartą modułu i formą zaliczenia. Cyberprzestrzeń – definicja, cechy.	2

W2	Ministerstwo Cyfryzacji – wizja, misja, wartości, zadania, dokumenty strategiczne, współpraca krajowa i międzynarodowa jako gwarancja cyberbezpieczeństwa	2
W3	Internet – powstanie i rozwój. Cyfryzacja nowych obszarów życia.	2
W4	Praca i nauka zdalna – rekomendacje bezpieczeństwa, typy zagrożeń w cyberprzestrzeni, minimalizacja ryzyka; sieci lokalne – elementy, wykorzystanie; usługi i udogodnienia Internetu. Internet rzeczy.	2
W5	E-społeczeństwo – dostępne programy, zalety i zagrożenia.	2
Warsztaty		
Kod	**Tematyka zajęć**	**Liczba godzin S**
WT1	Przedstawienie treści karty modułu. Incydent w systemie informatycznym. Identyfikacja, ocena konsekwencji, działania naprawcze, zapobiegawcze.	4
WT2	E społeczeństwo – dostępne programy.	4
WT3	Bezpieczne korzystanie z cyberprzestrzeni – zasady, zalecenia.	4
WT4	Dezinformacja, fake news, stalking, trollowanie – zagrożenia; edukacja jako narzędzie przeciwdziałania,	4
WT5	„W Internecie nic nie ginie" – sprawdź co wie o Tobie sieć. Bezpieczeństwo danych osobistych.	4

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia:
Wykład: informacyjny (konwencjonalny) prowadzony w formie konwencjonalnej lub zdalnie, np. on Line, problemowy, konwersatoryjny.
Warsztaty: metoda problemowa, metoda ćwiczeniowa oparta na wykorzystaniu różnych źródeł wiedzy, metoda projektu; tzw. burza mózgów, studium przypadku, dyskusja, analiza tekstów źródłowych.

2. Narzędzia (środki) dydaktyczne:
Sale komputerowe, prezentacje multimedialne, film, fotografie, materiały archiwalne, teksty źródłowe, dokumenty, Internet, rzutniki multimedialne, zajęcia zdalne

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

1. Formy zaliczenia:
- Wykłady – zaliczenie z oceną
- Warsztaty - zaliczenie z oceną

2. Sposób weryfikacji i oceniania efektów uczenia się:

Wykłady
- test wiedzy z pytaniami otwartym obejmujący swoim zakresem treści programowe zaprezentowane podczas wykładów, obserwacja i ocena postaw studenta.

Warsztaty
- udział i wykonywanie prac praktycznych w trakcie zajęć oraz przygotowanie prezentacji obrazującej realizację projektów o charakterze praktycznym

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

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

Warsztaty
- 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.

Kompetencje społeczne – obserwacja i ocena postaw studenta

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 warsztatach	20
Samodzielna praca studenta (godziny niekontaktowe)	**20**
Przygotowanie do wykładu	4
Przygotowanie do warsztatów	6
Przygotowanie do zaliczenia z oceną wykładu	4
Przygotowanie do zaliczenia z oceną warsztatów	6
Łączna liczba godzin	**50**
Punkty ECTS za moduł	**2**

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. J. Kosiński, Paradygmaty cyberprzestępczości; wyd. Difin SA, Warszawa 2015,
2. Praca zbiorowa pod red. J. Kosińskiego, *Przestępczość teleinformatyczna*; Wyd. WSPol Szczytno 2015
3. T. Trejderowski, *Kradzież tożsamości: terroryzm informatyczny: cyberprzestępstwa, Internet, telefon, Facebook;* wyd. Eneteia Wydawnictwo Psychologii i Kultury, Warszawa 2013