

**KARTA PRZEDMIOTU****I. Dane podstawowe**

Nazwa przedmiotu	Zagrożenia w cyberprzestrzeni
Nazwa przedmiotu w języku angielskim	Threats in Cyberspace
Kierunek studiów	Stosunki międzynarodowe
Poziom studiów (I, II, jednolite magisterskie)	II
Forma studiów (stacjonarne, niestacjonarne)	Stacjonarne
Dyscyplina	Nauki socjologiczne
Język wykładowy	Polski

Koordynator przedmiotu/osoba odpowiedzialna	Dr Alina Betlej
---	-----------------

Forma zajęć ( <i>katalog zamknięty ze słownika</i> )	Liczba godzin	semestr	Punkty ECTS
konwersatorium	30	I	2

Wymagania wstępne	W1-zainteresowanie problematyką; W2 - umiejętność analizowania tekstów naukowych
-------------------	---

**II. Cele kształcenia dla przedmiotu**

C1- Zapoznanie studentów ze współczesnymi zagrożeniami w cyberprzestrzeni.
C2- Przedstawienie studentom dylematów, wyzwań i zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

**III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych**

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
<b>WIEDZA</b>		
W_01	Student posiada wiedzę na temat współczesnych zagrożeń w cyberprzestrzeni	K_W01
W_02	Student zna dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii	K_W02
<b>UMIEJĘTNOŚCI</b>		
U_01	Student definiuje współczesne zagrożenia w cyberprzestrzeni	K_U02
U_02	Student porównuje i analizuje różne dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii	K_U01
<b>KOMPETENCJE SPOŁECZNE</b>		
K_01	Student jest wrażliwy na problemy bezpieczeństwa w cyberprzestrzeni	K_K06

K_02	Student jest świadomy zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii	K_K02
------	--	-------

#### IV. Opis przedmiotu/ treści programowe

<ol style="list-style-type: none"> <li>1. Wirtualizacja: wyzwania i skutki</li> <li>2. Bezpieczeństwo w sieci versus bezpieczeństwo sieci</li> <li>3. Manipulacja i propaganda</li> <li>4. Niechciane i nieodpowiednie treści</li> <li>5. Cyberprzemoc</li> <li>6. Przestępczość w sieci</li> <li>7. Uzależnienia w sieci</li> <li>8. Haktywizm versus aktywizm</li> <li>9. Cyberterroryzm</li> <li>10. Darknet</li> <li>11. Alternatywne społeczeństwo i alternatywna gospodarka?</li> <li>12. Społeczna ocena nowych technologii</li> <li>13. Scenariusze przyszłości</li> </ol>
--

#### V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne (lista wyboru)	Metody weryfikacji (lista wyboru)	Sposoby dokumentacji (lista wyboru)
<b>WIEDZA</b>			
W_01 – W_02	Dyskusja, praca w grupach, analiza studiów przypadków, przygotowanie wypowiedzi ustnej na wybrany temat	Ocena aktywności podczas konwersatorium, ocena prezentacji ustnej na wybrany temat	Protokół z zaliczenia
<b>UMIEJĘTNOŚCI</b>			
U_01 – U_02	Dyskusja, praca w grupach, analiza studiów przypadków, przygotowanie wypowiedzi ustnej na wybrany temat	Ocena aktywności podczas konwersatorium, ocena prezentacji ustnej na wybrany temat	Protokół z zaliczenia
<b>KOMPETENCJE SPOŁECZNE</b>			
K_02 – K_06	Dyskusja, praca w grupach, analiza studiów przypadków, przygotowanie wypowiedzi ustnej na wybrany temat	Ocena aktywności podczas konwersatorium, ocena prezentacji ustnej na wybrany temat	Protokół z zaliczenia

## **VI. Kryteria oceny, wagi**

Zaliczenie: odpowiedź ustna na wybrany temat

### **Na ocenę 2:**

**W**-Student nie posiada podstawowej wiedzy na temat współczesnych zagrożeń w cyberprzestrzeni. Student nie zna podstawowych dylematów, wyzwań i zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

**U**-Student nie definiuje wybranych współczesnych zagrożeń w cyberprzestrzeni. Student nie porównuje i nie analizuje wybranych dylematów, wyzwań i zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

**K**-Student nie jest wrażliwy na wybrane problemy bezpieczeństwa w cyberprzestrzeni. Student jest świadomy wybranych zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

### **Na ocenę 3:**

**W**-Student posiada podstawową wiedzę na temat współczesnych zagrożeń w cyberprzestrzeni.

Student zna podstawowe dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii.

**U**-Student definiuje wybrane współczesne zagrożenia w cyberprzestrzeni. Student porównuje i analizuje wybrane dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii.

**K**-Student jest wrażliwy na wybrane problemy bezpieczeństwa w cyberprzestrzeni. Student jest świadomy wybranych zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

### **Na ocenę 4:**

**W**-Student posiada dobrą wiedzę na temat współczesnych zagrożeń w cyberprzestrzeni.

Student zna wiele dylematów, wyzwań i zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

**U**-Student definiuje liczne współczesne zagrożenia w cyberprzestrzeni. Student porównuje i analizuje liczne dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii.

**K**-Student jest wrażliwy na problemy bezpieczeństwa w cyberprzestrzeni. Student jest świadomy zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

### **Na ocenę 5:**

**W**-Student posiada bardzo dobrą wiedzę na temat współczesnych zagrożeń w cyberprzestrzeni.

Student zna dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii.

**U**-Student definiuje współczesne zagrożenia w cyberprzestrzeni. Student porównuje i analizuje dylematy, wyzwania i zagrożenia dla porządku społecznego związane z rozwojem nowych technologii.

**K**-Student jest wrażliwy na problemy bezpieczeństwa w cyberprzestrzeni. Student jest świadomy zagrożeń dla porządku społecznego związanych z rozwojem nowych technologii.

**Obciążenie pracą studenta**

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	30
Liczba godzin indywidualnej pracy studenta	60

**VII. Literatura**

<b>Literatura podstawowa</b>
Betlej A., Society of e-control in Hyperconnected Reality, [in:] Transformations, nr 3-4 (94-95), p. 38-47.
Liedel K, Piasecka P., Aleksandrowicz T. R. (red.), Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, Difin 2014.
Podraza A., Potakowski P., Wiak K. (red.), Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin 2013.
Zacher L. W. (red.), Potencjały i relacje sił w cyfrowym społeczeństwie wiedzy, MT Biznes, Warszawa 2018.
<b>Literatura uzupełniająca</b>
Betlej A., Społeczeństwo sieciowe- relacje siły, [w:] L. W. Zacher (red.), Potencjały i relacje sił w cyfrowym społeczeństwie wiedzy, Wydawnictwo POLTEXT, Warszawa 2018, s.37-54.
Górka M. (red.), Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin 2014.