KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	Polityka cyberbezpieczeństwa
Nazwa przedmiotu w języku angielskim	Policy of Cybersecurity
Kierunek studiów	Bezpieczeństwo narodowe
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 *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład	15	I	3

Wymagania wstępne	W1- podstawowa wiedza z zakresu nowych technologii informacyjno-komunikacyjnych

II. Cele kształcenia dla przedmiotu

C1- Zapoznanie studentów z założeniami polityki cyberbezpieczeństwa
C2- Zapoznanie studentów z nowymi zagrożeniami związanymi z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni

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

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student zna założenia polityki cyberbezpieczeństwa	K_W01
W_02	Student zna zagrożenia związane z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni	K_W02
UMIEJĘTNOŚCI		
U_01	Student definiuje problemy cyberbezpieczeństwa w	K_U02

	cyfrowym świecie	
U_02	Student porównuje i analizuje różne studia przypadków cyberzagrożeń	K_U01
KOMPETENCJE SPOŁECZNE		
K_01	Student jest wrażliwy na problemy cyberbezpieczeństwa w cyfrowym świecie	K_K06, K_K02

IV. Opis przedmiotu/ treści programowe

1.Społeczeństwo informacyjne.

2.Bezpieczeństwo w cyberprzestrzeni.

3.Zagrożenia w sieciowym świecie.

4.Walka informacyjna, propaganda.

5.Haktywizm, cyfrowe podziemie.

6.Cyberterroryzm, cyberterror.

7.Cyberwojna.

8.Globalny wymiar cyberzagrożeń.

9.Globalny wymiar cyberbezpieczeństwa.

10.Instytucje zwalczające cyberzagrożenia.

11.Moje cyberbezpieczeństwo.

12.Cyberbezpieczeństwo w firmie.

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01 – W_02	Wykład konwencjonalny (MS Teams), wykład konwersatoryjny MS Teams)	Egzamin ustny, Odpowiedź ustna	Protokół z egzaminu
UMIEJĘTNOŚCI			
U_01 – U_02	Wykład problemowy MS Teams), wykład konwersatoryjny MS Teams)	Egzamin ustny, Odpowiedź ustna,	Protokół z egzaminu
KOMPETENCJE SPOŁECZNE			
K_02 –	Wykład problemowy MS	Egzamin ustny,	Protokół z egzaminu

K_06	Teams), wykład konwersatoryjny MS Teams)	Odpowiedź ustna	

VI. Kryteria oceny, wagi

Wykład: Egzamin ustny (MS Teams)

Ocena 2
W-Student nie zna założeń polityki cyberbezpieczeństwa. Student nie zna zagrożeń związanych z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni.
U- Student nie definiuje problemów cyberbezpieczeństwa w cyfrowym świecie. Student nie porównuje i nie analizuje różnych studiów przypadków cybezagrożeń.
K- Student nie jest wrażliwy na problemy cyberbezpieczeństwa w cyfrowym świecie.

Ocena 3
W-Student posiada podstawową wiedzę na temat wybranych założeń polityki cyberbezpieczeństwa. Student zna wybrane zagrożenia związane z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni.
U- Student definiuje wybrane problemy cyberbezpieczeństwa w cyfrowym świecie. Student porównuje i analizuje wybrane studia przypadków cybezagrożeń.
K- Student jest wrażliwy na wybrane problemy cyberbezpieczeństwa w cyfrowym świecie.

Ocena 4
W-Student zna wybrane założenia polityki cyberbezpieczeństwa. Student zna wybrane zagrożenia związane z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni.
U- Student definiuje wskazane przez Wykładowcę problemy cyberbezpieczeństwa w cyfrowym świecie. Student porównuje i analizuje wskazane przez Wykładowcę studia przypadków cybezagrożeń.
K- Student jest wrażliwy na wybrane problemy cyberbezpieczeństwa w cyfrowym świecie.

Ocena 5
W-Student zna założeni polityki cyberbezpieczeństwa. Student zna liczne zagrożenia związane z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni.
U- Student definiuje liczne problemy cyberbezpieczeństwa w cyfrowym świecie. Student porównuje i analizuje wiele studiów przypadków cybezagrożeń.
K- Student jest wrażliwy na problemy cyberbezpieczeństwa w cyfrowym świecie.

Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	15
Liczba godzin indywidualnej pracy studenta	90

VII. Literatura

Literatura podstawowa
Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018. Krawic J., *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019. Roman. A., *Testowanie i jakość oprogramowania. Modele, techniki, narzędzia*, Wydawnictwo Naukowe PWN, Warszawa 2017.
Literatura uzupełniająca
Górka M. (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Difin 2014.Raport PARP, Web Analytics, 2019.