

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

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

Forma zajęć (<i>katalog zamknięty ze słownika</i>)	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 cyfrowym świecie	K_U02
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

<p>1.Społeczeństwo informacyjne.</p> <p>2.Bezpieczeństwo w cyberprzestrzeni.</p> <p>3.Zagrożenia w sieciowym świecie.</p> <p>4.Walka informacyjna, propaganda.</p> <p>5.Haktywizm, cyfrowe podziemie.</p> <p>6.Cyberterroryzm, cyberterror.</p> <p>7.Cyberwojna.</p> <p>8.Globalny wymiar cyberzagrożeń.</p> <p>9.Globalny wymiar cyberbezpieczeństwa.</p> <p>10.Instytucje zwalczające cyberzagrożenia.</p> <p>11.Moje cyberbezpieczeństwo.</p> <p>12.Cyberbezpieczeństwo w firmie.</p>
--

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, wykład konwersatoryjny	Egzamin ustny, Odpowiedź ustna	Protokół z egzaminu
UMIEJĘTNOŚCI			
U_01 – U_02	Wykład problemowy, wykład konwersatoryjny	Egzamin ustny, Odpowiedź ustna,	Protokół z egzaminu
KOMPETENCJE SPOŁECZNE			
K_02 – K_06	Wykład problemowy, wykład konwersatoryjny	Egzamin ustny, Odpowiedź ustna	Protokół z egzaminu

VI. Kryteria oceny, wagi

Wykład: Egzamin ustny

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 cyberzagrożeń.

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 cyberzagrożeń.

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 cyberzagrożeń.

K- Student jest wrażliwy na wybrane problemy cyberbezpieczeństwa w cyfrowym świecie.

Ocena 5

W- Student zna założenia 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 cyberzagrożeń.

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.), <i>Cyberbezpieczeństwo. Zarys wykładu</i> , Warszawa 2018.
Krawic J., <i>Cyberbezpieczeństwo. Podejście systemowe</i> , 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.