KARTA PRZEDMIOTU DLA NABORU 2022/2023
FORMA STUDIÓW: STACJONARNA

INFORMACJE OGÓLNE

1. Nazwa przedmiotu Cyberzagrożenia bezpieczeństwa państwa

2. Nazwa kierunku Bezpieczeństwo Narodowe

3. Poziom kształcenia studia drugiego stopnia

4. Liczba punktów ECTS 3

5. Liczba godzin w semestrze

semestr	w	ćw	lab/lek	prj/zp	pws	prk
III	15	15				

6. Język wykładowy polski

7. Wykładowca dr Karol Dołęga, k.dolega@dyd.akademiabialska.pl

INFORMACJE SZCZEGÓŁOWE

8. Wymagania wstępne

brak

9. Cele przedmiotu

C1 Przekazanie studentom wiedzy dotyczącej problematyki cyberbezpieczeństwa.

C2 Zapoznanie studentów z polityką cyberbezpieczeństwa Polski i wybranych państw.

10. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot:		odniesienie do kierunkowych efektów uczenia się
	WIEDZA	
EU01	Definiuje podstawowe pojęcia z zakresu cyberprzestrzeni oraz ma wiedzę na temat jej specyfiki, uwarunkowań bezpieczeństwa w jej obszarze	K_W01, K_W02
EU02	Zna aspekty prawne związane z obszarem cyberbezpieczeństwa.	K_W12
	UMIEJĘTNOŚCI	
EU03	Analizuje, interpretuje i wyjaśnia bezpieczeństwo w cyberprzestrzeni, jego zagrożenia i działania na rzecz jego zapewnienia	K_U01, K_U04
	KOMPETENCJE SPOŁECZNE	
EU04	Ma potrzebę stałego pogłębiania wiedzy.	K_K01

11. Treści programowe

Forma zajęć – wykłady

1. Wprowadzenie do podstawowych pojęć związanych z cyberbezpieczeństwem.
2. Cyberprzestrzeń i jej ewolucja.

3. Uwarunkowania bezpieczeństwa w obszarze cyberprzestrzeni.
4. Prawne aspekty bezpieczeństwa w cyberprzestrzeni.
5. Zagrożenia w cyberprzestrzeni.
6. Strategia cyberbezpieczeństwa RP.
7. Rola i zadania kluczowych podmiotów publicznych zaangażowanych w aspekty krajowego systemu cyberbezpieczeństwa.
8. Działania służb specjalnych w zakresie zwalczania cyberzagrożeń.

Forma zajęć – ćwiczenia

1. Problematyka terminologiczna. Pojęcie cyberbezpieczeństwa.
2. Cyberbezpieczeństwo, rodzaje cyberzagrożeń.
3. Cyberprzestępczość.
4. Cyberterroryzm i jego zwalczanie.
5. Strategie bezpieczeństwa cyberprzestrzeni wybranych państw.
6. Strategia bezpieczeństwa cybernetycznego UE.
7. Wyzwania w cyberprzestrzeni.

12. Narzędzia/metody dydaktyczne

1. wykład
2. dyskusja
3. referat w postaci prezentacji multimedialnej

13. Sposoby oceny (cząstkowe, końcowe)

1. referat
2. kolokwium
3. zaliczenie

14. Obciążenie pracą studenta

Forma aktywności	liczba godzin
1. Zajęcia z bezpośrednim udziałem nauczyciela oraz konsultacje	42
2. Nakład pracy studenta – przygotowanie się do kolokwium i zaliczenia	17
3. Nakład pracy studenta – przygotowanie referatu w postaci prezentacji multimedialnej	16
suma	75
liczba punktów ECTS	**3**

15. Literatura

Literatura podstawowa:

1. Strategie cyberbezpieczeństwa
2. Krawiec J., Cyberbezpieczeństwo: podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2019.
3. Wojciechowska-Filipek S., Ciekanowski Z., Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki, organizacji, państwa, Warszawa 2015.
4. Górka M., Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku, Difin, Warszawa 2014.

Literatura uzupełniająca:

1. Liedel K., Piasecka P., Aleksandrowicz T. R., Bezpieczeństwo w XX wieku: asymetryczny świat, Difin, Warszawa 2011.
2. Sawicki M., Cyberprzestępczość, C.H. Beck, Warszawa 2013.
3. 3. Drmola J., Perspectives on cybersecurity, ebook, 2015.

16. Formy oceny – szczegóły
Ocena z wykładów – zaliczenie w postaci testu jednokrotnego wyboru (zaliczenie – minimum 51% punktów). Ocena z ćwiczeń – ocena wynikająca z sumy punktów z referatu i kolokwium (minimum 51% punktów).
17. Inne przydatne informacje o przedmiocie
1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela Prowadzący w trakcie zajęć i podczas konsultacji.
2. Zajęcia odbywają się w miejscu określonym w planie zajęć.
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć.
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem.