

KARTA PRZEDMIOTU DLA NABORU 2023/2024 FORMA STUDIÓW: NIESTACJONARNA						
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	9	9				
6. Język wykładowy język polski						
7. Wykładowca						
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	Jest gotów w sposób ciągły pogłębiać wiedzę.				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.	
<b>Forma zajęć – ćwiczenia</b>  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.	
<b>12. Narzędzia/metody dydaktyczne</b>	
1. wykład	
2. dyskusja	
3. referat w postaci prezentacji multimedialnej	
<b>13. Sposoby oceny (częstkowe, końcowe )</b>	
1. referat	
2. kolokwium	
3. zaliczenie	
<b>14. Obciążenie pracą studenta</b>	
Forma aktywności	liczba godzin
1. Zajęcia z bezpośrednim udziałem nauczyciela oraz konsultacje	30
2. Nakład pracy studenta – przygotowanie się do kolokwium i zaliczenia	25
3. Nakład pracy studenta – przygotowanie referatu w postaci prezentacji multimedialnej	20
suma	75
liczba punktów ECTS	3
<b>15. Literatura</b>	
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, organizacje, 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. Drmola J., Perspectives on cybersecurity, ebook, 2015.	

<b>16. Formy oceny – szczegóły</b>
<p>Ocena z wykładów – zaliczenie w postaci testu jednokrotnego wyboru (zaliczenie – minimum 51% punktów).</p> <p>Ocena z ćwiczeń – ocena wynikająca z sumy punktów z referatu i kolokwium (minimum 51% punktów).</p>
<b>17. Inne przydatne informacje o przedmiocie</b>
1. Informacja, gdzie można zapoznać się z materiałami do zajęć, itp. – na stronie Uczelni
2. Informacje na temat miejsca odbywania zajęć – w salach Uczelni
3. Informacja na temat terminu zajęć (dzień tygodnia/godzina) – zgodnie z planem zajęć umieszczonym na stronie Uczelni
4. Informacja na temat konsultacji (godziny + miejsce) – zgodnie z harmonogramem konsultacji umieszczonym na stronie Uczelni