

KARTA PRZEDMIOTU DLA NABORU 2023/2024 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@dud.akademiabialska.pl						
INFORMACJE SZCZEGÓŁOWE						
8. Wymagania wstępne						
Student powinien posiadać podstawowe wiadomości z zakresu wiedzy o społeczeństwie. Powinien posiadać umiejętność korzystania z różnych źródeł informacji.						
9. Cele przedmiotu						
C1 Zdobycie przez studentów wiedzy z zakresu cyberbezpieczeństwa, jego kluczowych zagrożeń oraz sposobów ich zwalczania.						
C2 Rozwój umiejętności analizy i syntezy oraz oceny i krytyki zjawisk związanych ze sferą cyberzagrożeń bezpieczeństwa państwa.						
C3 Zrozumienie przez studentów konieczności uczenia się przez całe życie oraz zrozumienie organizowania działań w grupie.						
10. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych						
Student, który zaliczył przedmiot:					odniesienie do kierunkowych efektów uczenia się	
WIEDZA						
EU01	Zna pojęcie cyberbezpieczeństwa oraz potrafi podać przykłady zagrożeń odnoszących się do bezpieczeństwa kulturowego i metody zapobiegania tymże zagrożeniom.				K_W02, K_W06	
EU02	Zna podstawy prawne cyberbezpieczeństwa państwa.				K_W04, K_W09	
UMIEJĘTNOŚCI						
EU03	Potrafi poddać analizie uwarunkowania bezpieczeństwa cybernetycznego państwa w aspekcie wewnętrznym i aspekcie zewnętrznym, ilustrując swoją wypowiedź przykładami.				K_U01, K_U04, K_U06, K_U19	
EU04	Potrafi krytycznie omówić relacje pomiędzy rodzajami bezpieczeństwa.				K_U01, K_U04, K_U06, K_U19	

KOMPETENCJE SPOŁECZNE		
EU05	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz problematyki współczesnego terroryzmu i zagrożeń asymetrycznych.	K_K01, K_K02
<b>11. Treści programowe</b>		
<b>Forma zajęć – wykłady</b> <ol style="list-style-type: none"> <li>1. Społeczeństwo informacyjne</li> <li>2. Cyberprzestrzeń i jej istota</li> <li>3. Technologia cyberprzestrzeni</li> <li>4. Zagrożenia w cyberprzestrzeni</li> <li>5. Podmioty cyberbezpieczeństwa</li> <li>6. Bezpieczeństwo państwa w cyberprzestrzeni – główne zagrożenia</li> <li>7. Rozwiązania prawno-instytucjonalne w zakresie bezpieczeństwa państwa w cyberprzestrzeni</li> </ol>		
<b>Forma zajęć – ćwiczenia</b> <ol style="list-style-type: none"> <li>1. Informacja i wiedza jako element funkcjonowania społeczeństwa informacyjnego</li> <li>2. Cyberprzestrzeń i jej ewolucja</li> <li>3. Wybrane cyberzagrożenia oraz ich zwalczanie</li> <li>4. Cyberterroryzm i jego zwalczanie</li> <li>5. Cyberprzestępczość</li> <li>6. System reagowania na incydenty komputerowe – wybrane aspekty</li> <li>7. Bezpieczeństwo cyberprzestrzeni w wymiarze instytucjonalnym</li> <li>8. Internet jako narzędzie propagandy</li> <li>9. Strategia Cyberbezpieczeństwa RP – analiza dokumentu</li> <li>10. Moje cyberbezpieczeństwo</li> <li>11. Wojna informacyjna</li> </ol>		
<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		42
2. Nakład pracy studenta – przygotowanie się do kolokwium i zaliczenia		11
3. Nakład pracy studenta – przygotowanie referatu w postaci prezentacji multimedialnej		22
suma		75
liczba punktów ECTS		3
<b>15. Literatura</b>		
Literatura podstawowa:		
1. P.Borek, Z. Ciekanowski, Determinanty bezpieczeństwa państwa wobec współczesnych zagrożeń, Biała Podlaska 2017.		
2. S. Wojciechowska-Filipek, Z. Ciekanowski , Bezpieczeństwo funkcjonowania w cyberprzestrzeni:		

jednostki, organizacji, państwa, Warszawa 2015.
3. T. Bąk, Z. Ciekanowski, T. Nowicka, Współczesne zagrożenia bezpieczeństwa państwa, Warszawa 2015.
4. A. Marczyk, Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, PRZEGŁĄD TELEINFORMATYCZNY NR 1-2, 2018.
5. J. Grubicka, E. Matuska, Bezpieczeństwo cyfrowe. Perspektywa organizacyjna, wyd. Difin, 2023.
6. M. Marczyk (red.), M. Stolarz (red.), B. Terebiński (red.), Bezpieczeństwo działań w cyberprzestrzeni. Wybrane Aspekty. Tom 1 Działania w cyberprzestrzeni i Tom 2 Techniczne aspekty cyberbezpieczeństwa, wyd. Akademii Sztuki Wojennej, 2022.
Literatura uzupełniająca:
1. W. Barszczewski, Cyberprzestrzeń jako obszar współczesnych zagrożeń [w:] Społeczeństwo jako uczestnik bezpieczeństwa. Wybrane zagadnienia, J. Nowicka (red.), ASZWOJ, Warszawa 2021 r.
2. K. Michalski, I. Oleksiewicz, E. Sienkiewicz, Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline, Warszawa 2017.
3. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.
4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
5. ENISA THREAT LANDSCAPE 2023, dostępne na stronie: <a href="https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends">https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends</a>
<b>16. Formy oceny – szczegóły</b>
<p>Student (-ka) zobowiązany jest do zaliczenia wykładu na ocenę w formie testu wielokrotnego wyboru będzie składał się z 30 pytań. Warunkiem uzyskania oceny pozytywnej jest uzyskanie 50% pozytywnych odpowiedzi.</p> <p>Punktacja – każde pytanie oceniane jest w skali od 0 do 1 pkt. Maksymalnie można uzyskać 30 pkt.</p> <ul style="list-style-type: none"> <li>• 0 – 14 pkt - niedostateczny (2,0)</li> <li>• 15 – 19 pkt - dostateczny (3,0)</li> <li>• 20 – 23 pkt - dostateczny plus (3,5)</li> <li>• 24 – 26 pkt - dobry (4,0)</li> <li>• 27 – 28 pkt - dobry plus (4,5)</li> <li>• 29 – 30 pkt - bardzo dobry (5,0)</li> </ul> <p>Student (-ka) zobowiązany jest do uzyskania zaliczenia ćwiczeń na ocenę. Warunkiem zaliczenia ćwiczeń jest przygotowanie prezentacji dotyczącej tytułowej tematyki, która oceniana jest w skali ocen 2-5 oraz kolokwium w formie testu wyboru (20 pytań). Treść pytań na kolokwium oparta jest o materiały przygotowane przez studentów w trakcie ćwiczeń. Warunkiem uzyskania oceny pozytywnej z kolokwium jest uzyskanie 50% pozytywnych odpowiedzi.</p> <p>Punktacja – każde pytanie oceniane jest w skali od 0 do 1 pkt. Maksymalnie można uzyskać 20 pkt.</p> <ul style="list-style-type: none"> <li>• 0 – 9 pkt - niedostateczny (2,0)</li> <li>• 10 – 12 pkt - dostateczny (3,0)</li> <li>• 13 – 14 pkt - dostateczny plus (3,5)</li> <li>• 15 – 16 pkt - dobry (4,0)</li> <li>• 17 – 18 pkt - dobry plus (4,5)</li> <li>• 19 – 20 pkt - bardzo dobry (5,0)</li> </ul> <p>Ponadto, w trakcie semestru student (-ka) może zdobyć punkty odzwierciedlające stopień aktywności na zajęciach.</p> <p>Ocenę końcową z ćwiczeń stanowi średnia ocena z prezentacji i kolokwium, która może być podwyższona za aktywność na zajęciach.</p>
<b>17. Inne przydatne informacje o przedmiocie</b>
1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela Prowadzący w trakcie zajęć i podczas konsultacji.
2. Zajęcia odbywać się będą w salach Akademii Białskiej.
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć.
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem.

