

KARTA PRZEDMIOTU								
Kod przedmiotu		BNPM208						
Nazwa przedmiotu		AKTUALNE PROBLEMY BEZPIECZEŃSTWA W CYBERPRZESTRZENI						
USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW								
Kierunek studiów		BEZPIECZEŃSTWO NARODOWE						
Forma studiów		niestacjonarne						
Poziom studiów		drugiego stopnia/magisterskie						
Profil studiów		praktyczny						
Dziedzina kształcenia		dziedzina nauk społecznych/ dyscyplina naukowa: nauki o bezpieczeństwie, nauki o polityce i administracji, nauki prawne						
Jednostka prowadząca przedmiot		Bydgoska Szkoła Wyższa						
Osoby prowadzące przedmiot		mgr inż. Radosław Jaroszewski						
OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU								
Status przedmiotu		obowiązkowy						
Przynależność do modułu		moduł podstawowy						
Język wykładowy		polski						
Semestry, na których realizowany jest przedmiot		drugi						
Wymagania wstępne		Wykład i ćwiczenia - ogólna wiedza z zakresu obsługi komputera						
FORMY, SPOSOBY I METODY PROWADZENIA ZAJĘĆ								
Formy zajęć	wykład	ćwiczenia	seminarium	laboratorium	projekt/prezentacja	praktyka	samokształcenie	ECTS
Liczba godzin	10	10	---	---	---	---	55	3
Sposób realizacji zajęć		wykład / ćwiczenia						
Sposób zaliczenia zajęć		wykład : zaliczenie pisemne (test i zadania on line) ćwiczenia : zaliczenie pisemne (test i zadania on line)						
Metody dydaktyczne		wykład – wykład informacyjny/ wykład problemowy ćwiczenia – ćwiczeniowa (oparta na wykorzystaniu różnych źródeł wiedzy, m.in. Internet)						
Wykaz literatury								
podstawowa		1. Bałut D., Budek K. (2018), <a href="https://marketingibiznes.pl/it/cyberbezpieczenstwo/">https://marketingibiznes.pl/it/cyberbezpieczenstwo/</a> 2. CERT POLSKA <a href="https://www.cert.pl">https://www.cert.pl</a> 3. Portal Niebezpiecznik <a href="https://www.cert.pl">https://www.cert.pl</a> 4. Portal <a href="https://zaufanatrzeciastrona.pl/">https://zaufanatrzeciastrona.pl/</a>						
uzupełniająca		1. Gołębiowski D., <i>Twoje bezpieczeństwo w świecie cyber i AI, Część I – wprowadzenie</i> , 2025. 2. Marczyk M., Stolarz M., Terebiński B., <i>Cyberbezpieczeństwo – zagrożenia i wyzwania</i> , Warszawa 2023. 3. Rojszczak M., Banasiński C., <i>Cyberbezpieczeństwo</i> , 2021. 4. Vacca J. R., <i>Computer and Information Security Handbook</i> , 3rd Edition, Morgan Kaufmann, 2017. 5. Conklin, A., White, G., Cothren, C., Davis, R., Williams, D., <i>Principles of Computer Security</i> . CompTIA Security+ and 3.						

	6. Beyond, Fifth Edition, McGraw-Hill, 2018 7. <i>Strategia cyberbezpieczeństwa.</i>
--	---

CELE, TREŚCI I EFEKTY UCZENIA SIĘ	
Cele przedmiotu	
Cel 1	Zapoznanie studentów z zagadnieniami związanymi aktualnymi zagrożeniami w cyberprzestrzeni.
Cel 2	Przygotowanie studentów do umiejętnego poszukiwania i przeciwdziałania nowym zagrożeniom z cyberprzestrzeni.

Treści programowe		
FORMA WYKŁADOWA		
	Liczba godzin	Treści programowe
wykłady	10 godz.	<ul style="list-style-type: none"> <li>— Cyberprzestrzeń</li> <li>— Wirtualna rzeczywistość</li> <li>— Polityka ochrony Cyberprzestrzeni RP</li> <li>— Definicje istotne dla cyberbezpieczeństwa</li> <li>— Bezpieczeństwo portali administracji rządowej</li> <li>— Zagrożenia i podatności</li> <li>— Infekcja, kradzież i gromadzenie danych, jak się chronić.</li> <li>— System ARAKIS-GOV</li> <li>— Inżynieria społeczna</li> <li>— Kampanie phishingowe</li> <li>— Rozwój Darknetu i wzrost aktywności cyberterrorystów</li> <li>— Zasady bezpieczeństwa w sieciach i systemach komputerowych</li> <li>— Metody bezpiecznego uwierzytelniania</li> </ul>
ćwiczenia	10 godz.	<ul style="list-style-type: none"> <li>— Przykłady ataków na sieci i systemy komputerowe</li> <li>— Ochrona systemów i sieci komputerowych -łatanie systemów</li> <li>— Złośliwe oprogramowanie – kategorie zagrożeń</li> <li>— Najczęstsze działania ze strony malware'u</li> <li>— Klasyfikacja ataków według CERT</li> <li>— Firewall</li> <li>— Systemy ochrony przed intruzami</li> <li>— Wykrywanie ataków sieciowych</li> <li>— Bezpieczna komunikacja w sieci i systemach</li> </ul> <p>W ramach realizacji zajęć realizowany jest wyjazd studyjny do Ministerstwa Cyfryzacji.</p>

Efekty uczenia się				
	Student, który zaliczył przedmiot	Odniesienie do efektów uczenia się		
	w zakresie WIEDZY	dla kierunku	UCh I st. PRK poziom 7	Ch II st. PRK poziom 7
EU1	ma pogłębioną i poszerzoną o innowacyjne aspekty wiedzę na temat znaczenia pojęć związanych z aktualnymi problemami w cyberprzestrzeni w kontekście bezpieczeństwa państwa	K_W03 K_W06	P7U_W	P7S_WG
EU2	zna źródła wyszukiwania zagrożeń w kontekście bezpieczeństwa państwa, rozumie ich znaczenie dla funkcjonowania współczesnego państwa i bezpieczeństwa	K_W03 K_W06	P7U_W	P7S_WG
w zakresie UMIEJĘTNOŚCI				
EU3	wyszukuje, obserwuje oraz właściwie interpretuje informacje na temat zagrożeń w cyberprzestrzeni, wskazuje najważniejsze aktualne wyzwania cyberbezpieczeństwa	K_U03 K_U04 K_U07	P7U_U	P7S_UW
EU4	analizuje zagrożenia dla systemów operacyjnych i sieci i wykorzystuje w celu przeciwdziałania im zaawansowane techniki informacyjno – komunikacyjne (ICT)	K_U03 K_U04 K_U07	P7U_U	P7S_UW
EU5	potrafi dokonać krytycznej analizy modelowych rozwiązań strategii cyberbezpieczeństwa, pogłębia i uzupełnia wiedzę, planuje i realizuje proces dalszego uczenia się	K_U02 K_U03 K_U04 K_U07	P7U_U	P7S_UW
EU6	Potrafi realizować zadania zawodowe w kwestii cyberbezpieczeństwa indywidualnie i w pracy zespołowej, ma świadomość konieczności podnoszenia swoich kwalifikacji w analizowanym zakresie	K_U09 K_U10	P7U_U	P7S_UO P7S_UU

w zakresie KOMPETENCJI				
EU7	ma świadomość odpowiedzialności za wykonywaną pracę zawodową, jest ukierunkowany na profesjonalne wykonywanie obowiązków zawodowych, jednocześnie ukierunkowuje się na dzielenie się wiedzą z innymi osobami	K_K06	P7K_K	P7S_KR

Kryteria oceny osiągniętych efektów	
na ocenę 2	poniżej 51% - opanowanie wiedzy na poziomie poniżej zadowalającego, brak podstawowej wiedzy w zakresie realizowanej tematyki
na ocenę 3	51-60% - opanowanie na poziomie zadowalającym podstawowych kwestii wynikających z treści programowych
na ocenę 3,5	61-70% - przyswojenie na średnim poziomie problematyki aktualnych problemów bezpieczeństwa w cyberprzestrzeni
na ocenę 4	71-80% - uzyskanie wiedzy co do czynników kształtujących podstawowe zjawiska z zakresu aktualnych problemów bezpieczeństwa w cyberprzestrzeni
na ocenę 4,5	81-90% - kompleksowe opanowanie treści programowych umożliwiające identyfikację zasad teoretycznych i praktycznych aspektów funkcjonowania aktualnych problemów bezpieczeństwa w cyberprzestrzeni
na ocenę 5	91-100% - doskonale, zaawansowane opanowanie treści programowych w tym części dotyczącej rozwiązywania problemów związanych z zastosowaniem wiedzy na temat aktualnych problemów bezpieczeństwa w cyberprzestrzeni

Metody oceny
<b>Ocena formułująca</b> F2. Pytania zadawane przez studenta świadczące o poziomie wiedzy i zainteresowania problematyką F4. Przygotowanie wcześniejsze materiału i zaprezentowanie go przez studenta na zajęciach
<b>Ocena podsumowująca P</b> P1. Ocena z wypowiedzi zaliczającej ćwiczenia – test on-line(ćwiczenia) P4. Ocena z zaliczenia końcowego – test on-line (wykład)

METODY (SPOSOBY) WERYFIKACJI I OCENY ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ OSIĄGNIĘTYCH PRZEZ STUDENTA						
Efekt uczenia się	Forma oceny					
	Egzamin ustny	Zaliczenie pisemne – test on-line/ wykład	Zaliczenie pisemne – test on-line/ ćwiczenia	rozwiązywanie zadań praktycznych	sprawozdanie	inne
EU 1		X				
EU 2		X				
EU 3			X			
EU 4			X			
EU 5			X			
EU 6			X			
EU 7		X	X			

zaliczenie końcowe	praktyczna forma zaliczenia (test i zadania on line)
zaliczenie końcowe	praktyczna forma zaliczenia (test i zadania on line)

Obciążenie pracą studenta - bilans punktów ECTS			
Forma aktywności		Obciążenie studenta	
		Godziny	ECTS
Godziny kontaktowe z nauczycielem akademickim, w tym:			
Godziny wynikające z planu studiów	wykłady	10	0,4
	ćwiczenia	10	0,4
	inne	-	-
Razem		20	0,8
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym			
przygotowanie do egzaminu/ zaliczenia		10	0,4

końcowego/zdawanie egzaminu/zaliczenia końcowego		
przygotowanie do kolokwίων/ odpowiedzi ustnej	-	-
przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10	<b>0,4</b>
przygotowanie raportu, projektu, prezentacji, dyskusji	10	<b>0,4</b>
<b>Razem</b>	<b>30</b>	<b>1,2</b>
<b>Razem PRZEDMIOT</b>	<b>50</b>	<b>2,0</b>

<b>Bilans punktów ECTS</b>					
ECTS/ WYKŁAD	ECTS/ ĆWICZENIA	ECTS/ LABORATORIUM	ECTS/ PRACOWNIA/ PROJEKT	ECTS/ SEMINARIUM	ECTS/ SUMA
<b>1</b>	<b>1</b>	-	-	-	<b>2</b>