

KARTA PRZEDMIOTU								
Kod przedmiotu		BNPL308						
Nazwa przedmiotu		CYBERBEZPIECZEŃSTWO						
USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW								
Kierunek studiów		BEZPIECZEŃSTWO NARODOWE						
Forma studiów		niestacjonarne						
Poziom studiów		pierwszego stopnia/licencjackie						
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		czwarty						
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 online) ćwiczenia – zajęcia interaktywne – praktyczne – rozwiązanie zadania praktycznego związanego z cyberzagrożeniami (test online)						
Metody dydaktyczne		wykład – wykład informacyjny/ wykład problemowy						
Wykaz literatury								
podstawowa		1. Bałut D., Budek K. (2018), https://marketingibiznes.pl/it/cyberbezpieczenstwo/ 2. CERT POLSKA https://www.cert.pl 3. Portal Niebezpiecznik https://www.cert.pl 4. Portal https://zaufanatrzeciastrona.pl/						
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+ and3.						

	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 podstawowymi zagadnieniami związanymi z zapewnianiem ochrony w obszarze cyberprzestrzeni
Cel 2	Przygotowanie studentów do ochrony przestrzeni informacji i zachodzących interakcji w sieciach i systemach informatycznych.

Treści programowe		
FORMA WYKŁADOWA		
	Liczba godzin	Treści programowe
wykłady	10 godz.	<ul style="list-style-type: none"> — Jak zrozumieć pojęcie cyberbezpieczeństwa? — Prawne i społeczne aspekty cyberbezpieczeństwa — Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. — Cyberbezpieczeństwo, czyli jak zapewnić tajność dokumentów w firmie. — Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. — Strategia cyberbezpieczeństwa — Włamania do systemów informatycznych, ataki sieciowe, ataki na użytkowników końcowych, socjotechnika
FORMA ĆWICZENIA		
ćwiczenia	10 godz.	<ul style="list-style-type: none"> — Rodzaje cyberataków - case study — Cyberbezpieczeństwo w wymiarze cyberprzestrzeni - case study — Cyberbezpieczeństwo w ujęciu danych osobowych - case study — Cyberbezpieczeństwo informacji niejawnych - case study

Efekty uczenia się				
	Student, który zaliczył przedmiot	Odniesienie do efektów uczenia się		
	w zakresie WIEDZY	dla kierunku	UCh I st. PRK poziom 6	Ch II st. PRK poziom 6
EU1	ma wiedzę na temat znaczenia cyberbezpieczeństwa w kontekście bezpieczeństwa państwa	K_W05	P6U_W	P6S_WG
EU2	wszechstronnie zna i dogłębnie rozumie stanowisko współczesnej nauki prawa, w szczególności prawa europejskiego w kontekście ustalenia zasad cyberbezpieczeństwa usług kluczowych i usług cyfrowych stosuje nowe rozwiązania – metody, techniki i narzędzia badawcze pozwalające na utrzymanie właściwego poziomu cyberbezpieczeństwa	K_W06 K_W07	P6U_W	P6S_WG
w zakresie UMIEJĘTNOŚCI				
EU3	interpretuje i stosuje w praktyce przepisy związane z zapewnieniem cyberbezpieczeństwa	K_U04	P6U_U	P6S_UW
EU4	analizuje zagrożenia dla systemów operacyjnych i sieci i wykorzystuje w celu przeciwdziałania im zaawansowane techniki informacyjno – komunikacyjne (ICT)	K_U05 K_U07	P6U_U	P6S_UK
EU5	współdziała w zespołach multidyscyplinarnych dla zapewnienia realizacji zadań związanych z zapewnieniem cyberbezpieczeństwa, dla osiągnięcia zakładanego celu	K_U12	P6U_U	P6S_UO
EU6	pogłębia i uzupełnia wiedzę, planuje i realizuje proces dalszego uczenia się	K_U13	P6U_U	P6S_UU
w zakresie KOMPETENCJI				
EU7	ma świadomość odpowiedzialności za wykonywaną pracę zawodową, jest ukierunkowany na profesjonalne wykonywanie obowiązków zawodowych	K_K01	P6K_K	P6S_KK

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 cyberbezpieczeństwa
na ocenę 4	71-80% - uzyskanie wiedzy co do czynników kształtujących podstawowe zjawiska z zakresu cyberbezpieczeństwa
na ocenę 4,5	81-90% - kompleksowe opanowanie treści programowych umożliwiające identyfikację zasad teoretycznych i praktycznych aspektów funkcjonowania cyberbezpieczeństwa
na ocenę 5	91-100% - doskonałe, zaawansowane opanowanie treści programowych w tym części dotyczącej rozwiązywania problemów związanych z zastosowaniem wiedzy na temat cyberbezpieczeństwa

Metody oceny
Ocena formułująca F2. Pytania zadawane przez studenta świadczące o poziomie wiedzy i zainteresowania problematyką F4. Przygotowanie wcześniejsze materiału i zaprezentowanie go przez studenta na zajęciach
Ocena podsumowująca P P2. Ocena z kolokwium kończącego przedmiot (wykład) P4. Ocena z zaliczenia końcowego (wykład)

METODY (SPOSOBY) WERYFIKACJI I OCENY ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ OSIĄGNIĘTYCH PRZEZ STUDENTA						
Efekt uczenia się	Forma oceny					
	wykład		ćwiczenia			
	Zaliczenie pisemne – test online	Zaliczenie ustne/ Egzamin ustny	Zaliczenie ćwiczeń – test online	rozwiązywanie zadań / ćwiczenia – case study	Kolokwia/ ćwiczenia	Obecność i aktywność na zajęciach / ćwiczenia
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 – wykład)
zaliczenie końcowe	praktyczna forma zaliczenia (zadania - case study - ćwiczenia)- test online

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
Razem		20	0,8
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym			
przygotowanie do egzaminu/ zaliczenia końcowego/zdanie egzaminu/zaliczenia końcowego		20	0,8
przygotowanie do kolokwium/ odpowiedzi ustnej		-	-
przygotowanie się do zajęć, w tym studiowanie zalecanej literatury		25	1,0

przygotowanie raportu, projektu, prezentacji, dyskusji	10	0,4
Razem	55	2,2
Razem PRZEDMIOT	75	3,0

Bilans punktów ECTS					
ECTS/ WYKŁAD	ECTS/ ĆWICZENIA	ECTS/ LABORATORIUM	ECTS/ PRACOWNIA/ PROJEKT	ECTS/ SEMINARIUM	ECTS/ SUMA
2	1	-	-	-	3