

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo informacyjne (Ćw. audytoryjne), PG_00205615						
Kierunek studiów	Bezpieczeństwo narodowe (P)						
Data rozpoczęcia studiów	październik 2027 r.		Rok akademicki realizacji przedmiotu		2027/2028		
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z praktycznym przygotowaniem zawodowym - profil praktyczny		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		polski		
Semestr studiów	2		Liczba punktów ECTS		2.0		
Profil kształcenia	praktyczny		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Rada Uczelni						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Konrad Ćwikliński				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	0.0	30.0	0.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30		0.0		20.0	50
Cel przedmiotu	Celem przedmiotu Bezpieczeństwo informacyjne w formie ćwiczeń audytoryjnych jest przygotowanie studentów do rozumienia, analizowania i praktycznego rozwiązywania problemów związanych z bezpieczeństwem informacji w kontekście funkcjonowania państwa, instytucji publicznych oraz podmiotów prywatnych. Przedmiot ma na celu wykształcenie umiejętności identyfikacji zagrożeń informacyjnych, oceny ryzyka oraz stosowania środków zaradczych, w tym organizacyjnych, technicznych i prawnych. Szczególny nacisk położony zostanie na rozwijanie kompetencji w zakresie ochrony danych, cyberbezpieczeństwa, zarządzania incydentami bezpieczeństwa oraz analizowania współczesnych zagrożeń hybrydowych i dezinformacyjnych. W ramach ćwiczeń studenci zapoznają się z praktycznymi aspektami bezpieczeństwa informacyjnego od podstaw analizy informacji i oceny wiarygodności źródeł, przez modelowanie zagrożeń, po opracowanie procedur reagowania i zabezpieczania systemów informacyjnych. Ćwiczenia obejmują analizę rzeczywistych przypadków naruszeń bezpieczeństwa, tworzenie planów bezpieczeństwa informacyjnego, a także rozwiązywanie zadań symulacyjnych i problemowych.						

Efekty uczenia się przedmiotu	Effekt kierunkowy	Effekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[BNL3_K04] Jest przygotowana do aktywności na rynku pracy, ma świadomość konieczności podnoszenia kwalifikacji odpowiedzialnego pełnienia ról zawodowych.	Jest przygotowany do pracy w sektorze ochrony informacji i rozumie potrzebę ciągłego doskonalenia zawodowego.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK2] prezentacja/projekt/referat/ raport
	[BNL3_U02] Analizuje przyczyny i przebieg procesów oraz ich ewolucji odnoszących się do społecznych, politycznych, ekonomicznych, prawnych, etycznych i kulturowych aspektów bezpieczeństwa.	Analizuje przyczyny i skutki procesów zagrożeń informacyjnych w kontekście społecznym, politycznym i prawnym.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
	[BNL3_U05] Wskazuje i wyjaśnia rolę państwa demokratycznego, a także społeczeństwa obywatelskiego w obszarze bezpieczeństwa.	Wyjaśnia rolę instytucji demokratycznych w zapewnianiu bezpieczeństwa informacyjnego.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
	[BNL3_U07] Aktywnie uczestniczy w życiu społeczno-politycznym oraz podejmuje próby uczestnictwa w dyskursie publicznym. Kieruje procesem samokształcenia rozwija swój warsztat pracy oraz nowe umiejętności poznawcze. Planuje i organizuje pracę swoją i zespołu, przygotowując projekty społeczne, polityczne, ekonomiczne, obywatelskie (także te, które polegają na współdziałaniu z innymi osobami), korzystając z różnych źródeł i możliwości technologicznych.	Uczestniczy w projektach dotyczących bezpieczeństwa informacyjnego, wykorzystując źródła cyfrowe i narzędzia technologiczne.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
	[BNL3_W13] Posiada wiedzę z zakresu prawa własności intelektualnej, obejmującą ochronę praw autorskich oraz własności przemysłowej.	Student zna i rozumie zasady prawa autorskiego oraz ochrony własności intelektualnej w systemach informacyjnych.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport
	[BNL3_W08] W zaawansowanym stopniu wie jakie są mechanizmy w zarządzaniu ryzykiem i podejmowaniu decyzji w instytucjach bezpieczeństwa narodowego.	Posiada wiedzę o funkcjonowaniu państwa i społeczeństwa w kontekście ochrony informacji i cyberbezpieczeństwa	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport
Treści przedmiotu	Ramowy program przedmiotu (ćwiczenia audytoryjne) <ol style="list-style-type: none"> 1. Wprowadzenie do przedmiotu. Podstawowe pojęcia bezpieczeństwa informacji. 2. Klasyfikacja informacji. Ochrona informacji niejawnych i wrażliwych. 3. Źródła i typy zagrożeń informacyjnych. Przykłady cyberataków. 4. Analiza ryzyka. Metody i matryce oceny ryzyka. 5. Zarządzanie incydentami. Reagowanie i raportowanie. 6. Polityka bezpieczeństwa informacji. Tworzenie dokumentu. 7. Ochrona danych osobowych. Prawo autorskie i IP. 8. Audyt bezpieczeństwa informacji zasady i etapy. 9. Narzędzia audytorskie. Praca z checklistą i dokumentacją. 10. Systemy ISMS. Norma ISO/IEC 27001. 11. Inżynieria społeczna. Czynniki ludzkie w zagrożeniach. 12. Cyberbezpieczeństwo a bezpieczeństwo informacyjne. 13. Etyka i odpowiedzialność. Rola sygnalistów (whistleblowing). 14. Projekt audytu praca zespołowa. 15. Prezentacja projektów.. Podsumowanie. 		
Wymagania wstępne i dodatkowe			

Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)		
	Praca w grupach		Próg zaliczeniowy
	Aktywność w zajęciach		Składowa oceny końcowej
Zalecana lista lektur	Podstawowa lista lektur		50.0%
	Uzupełniająca lista lektur		50.0%
	Adresy eZasobów		65.0%
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> Co to jest analiza ryzyka w bezpieczeństwie informacji? Jakie są różnice między polityką bezpieczeństwa a procedurami operacyjnymi? Wymień podstawowe elementy systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001. Jakie są typowe zagrożenia w systemach informacyjnych? Jakie znaczenie ma człowiek w systemie bezpieczeństwa informacji? 		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.