

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo - wykład, PG_00131767						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu			2028/2029		
Poziom kształcenia	I stopnia - licencjackie	Grupa zajęć			Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	3	Język wykładowy			polski		
Semestr studiów	6	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji -> Katedra Informatyki Prawniczej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	mgr Patryk Ciurak					
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	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	Uzyskanie wiedzy i umiejętności niezbędnych do opracowania projektów i strategii ograniczania ryzyka cybernetycznego, w tym odpowiednich kroków prawnych, które należy podjąć w odpowiedzi na ataki cybernetyczne. Dogłębne zrozumienie różnych rodzajów ataków cybernetycznych, na które są narażone systemy informacyjne biznesu i administracji. Poznanie roli i znaczenia podejścia do bezpieczeństwa cybernetycznego w całej organizacji opartego na ocenie ryzyka.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu			Sposób weryfikacji i oceny efektu	
	[KRYML3_W04] Posiada zaawansowaną wiedzę oraz rozumie uwarunkowania prawne i instytucjonalne funkcjonowania organów państwowych, a także rolę organów państwowych w przeciwdziałaniu zjawiskom patologicznym, zwłaszcza przestępstwom, zna także strukturę wewnętrzną tych organów i ich kompetencje		Student. 1. Zna obowiązki i uprawnienia podmiotów państwowych i prywatnych wynikające z wykorzystywania nowych technologii informacyjnych i komunikacyjnych. 2. Wie jakie działania należy podejmować ograniczając zagrożenia pochodzące z cyberprzestrzeni.			[SW4] test/egzamin - ustny lub pisemny [SW3] opracowanie tekstowe/praca pisemna [SW5] realizacja zadania problemowego	
	[KRYML3_W03] Posiada zaawansowaną wiedzę oraz rozumie zależności i uwarunkowania społeczne i psychologiczne między wybranymi zjawiskami związanymi z problematyką czynu zabronionego, w tym na temat kluczowych zjawisk społecznych i psychologicznych, istotnych w kontekście studiowanego kierunku		Student: 1. Zachowuje podstawowe zasady cyberhigieny w środowisku pracy i w miejscu zamieszkania. 2. Potrafi służyć poradą w kwestiach bezpieczeństwa informacyjnego. 3. Rozumie skomplikowane, interdyscyplinarne zależności związane ze funkcjonowaniem krajowego systemu cyberbezpieczeństwa			[SW4] test/egzamin - ustny lub pisemny [SW3] opracowanie tekstowe/praca pisemna [SW5] realizacja zadania problemowego	

Treści przedmiotu	1. Podstawowe pojęcia związane z cyberbezpieczeństwem. 2. Cyberprzestrzeń a Internet 3. Prawne modele regulacji cyberprzestrzeni 4. Regulacja Internetu 5. Sieci komputerowe i podstawowe kategorie cyberprzestępstw 6. Unijny system cyberbezpieczeństwa. Ramy prawne 7. Cyberhigiena		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Pisemne rozwiązanie zagadnienia problemowego	51.0%	100.0%
Zalecana lista lektur	Podstawowa lista lektur	1. C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu, wyd. 2. Wolters Kluwer, Warszawa 2023 2. K. Czaplicki, A. Gryszczyńska, G. Szpor [red.:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, Warszawa 2019	
	Uzupełniająca lista lektur	1. F. Wołowski, J. Zawila-Niedźwiecki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków 2012; 2. J. Łuczak, M. Tyburski, Systemowe zarządzanie bezpieczeństwem informacji wg ISO/IEC 27001:2005, Wyd. UE, Poznań 2009; 3. K. Liderman, Bezpieczeństwo informacyjne : nowe wyzwania, Warszawa, 2017 4. D. Szostek [red.:] Bezpieczeństwo danych i IT w kancelarii prawnej/ radcowskiej/adwokackiej/notarialnej/ komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej C.H.Beck, Warszawa 2018; 5. D. Lisiak-Felicka, M. Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, European Association For Security, Kraków 2016, https://www.researchgate.net/publication/301204372_Cyberbezpieczenstwo_administracji_publicznej_w_Polsce_download 6. M. Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, European Association For Security, Kraków 2014; 7. N. Polemi, Port Cybersecurity. Securing critical information infrastructures and supply chains, Elsevier, Amsterdam-Oksford-Cambridge 2018; 8. J. Kossoff, Cybersecurity Law, Wiley, Hoboken 2020.	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.