

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo - wykład, PG_00134172						
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		
Forma studiów	niestacjonarne	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	15.0	0.0	0.0	0.0	0.0	15
	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	15		0.0		35.0	50
Cel przedmiotu	<p>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.</p>						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[KRYML3_UU03] W zaawansowanym stopniu potrafi samodzielnie zdobywać wiedzę i rozwijać swoje profesjonalne umiejętności, korzystając z różnych źródeł (w języku rodzimym i obcym) i nowoczesnych technologii oraz odpowiednio dobierać i stosować właściwe metody i narzędzia pracy kryminologa	Student: 1. Zna podstawowe sposoby zapobiegania atakom na systemy informacyjne, zwalczania takich ataków, zabezpieczania dowodów i raportowania incydentów bezpieczeństwa. 2. Umie wykonać analizę ryzyka systemy, stanowiska roboczego, organizacji i procesu. 3. Umie analizować i rozumie informacje związanych z obowiązkami nałożonymi na najważniejszych aktorów funkcjonujących w obszarze cyberbezpieczeństwa. 4. Potrafi stosować w praktyce mechanizmy działania krajowego systemu cyberbezpieczeństwa.	[SU3] opracowanie tekstowe/praca pisemna [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego
	[KRYML3_WG04] Posiada zaawansowaną wiedzę na temat roli organów państwowych w przeciwdziałaniu zjawiskom społeczнопатologicznym, zwłaszcza przestępstwom, strukturze wewnętrznej tych organów i ich kompetencjach	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_WG03] Posiada zaawansowaną wiedzę na temat faktów, pojęć i zależności 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	C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu, wyd. 2. Wolters Kluwer, Warszawa 2023 K. Czaplicki, A. Gryszczyńska, G. Szpor [red.:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, Warszawa 2019	

	Uzupełniająca lista lektur	<ol style="list-style-type: none"> 1. <i>F. Wołowski, J. Zawila-Niedźwiecki</i>, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków 2012; 2. <i>J. Łuczak, M. Tyburski</i>, Systemowe zarządzanie bezpieczeństwem informacji wg ISO/IEC 27001:2005, Wyd. UE, Poznań 2009; 3. <i>K. Liderman</i>, Bezpieczeństwo informacyjne : nowe wyzwania, Warszawa, 2017 4. <i>D. Szostek [red.]</i> 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. <i>D. Lisiak-Felicka, M. Szmít</i>, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, European Association For Security, Kraków 2016, https://www.researchgate.net/publication/301204372_Cyberbezpieczenstwo_administracji_publicznej_w_Polsce 6. <i>M. Szmít</i>, Wybrane zagadnienia opiniowania sądowo-informatycznego, European Association For Security, Kraków 2014; 7. <i>N. Polemi</i>, Port Cybersecurity. Securing critical information infrastructures and supply chains, Elsevier, Amsterdam-Oksford-Cambridge 2018; 8. <i>J. Kossoff</i>, 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.