

Karta przedmiotu

Nazwa i kod przedmiotu	Seminarium III - ROJSZCZAK Marcin, PG_00198671						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2026 r.		Rok akademicki realizacji przedmiotu		2027/2028		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć fakultatywnych		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski		
Semestr studiów	4		Liczba punktów ECTS		4.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji -> Katedra Informatyki Prawniczej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr hab. Marcin Rojszczak				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	0.0	0.0	0.0	0.0	30.0	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		70.0	100
Cel przedmiotu	Celem seminarium jest przygotowanie studenta do samodzielnego opracowania pracy magisterskiej dotyczącej problematyki prawa nowych technologii, ze szczególnym uwzględnieniem prawnych i kryminologicznych aspektów cyberbezpieczeństwa, cyberprzestępczości oraz regulacji nowych i przełomowych technologii. Seminarium służy rozwijaniu umiejętności identyfikowania i formułowania problemów badawczych, krytycznej analizy źródeł prawa, orzecznictwa i literatury naukowej, doboru właściwych metod badawczych oraz konstruowania i prezentowania argumentacji naukowej. W toku seminarium student, we współpracy z promotorem, określa i doprecyzowuje przedmiot badań, formułuje problem i pytania badawcze, gromadzi oraz analizuje materiał źródłowy, przygotowuje strukturę pracy, a następnie opracowuje i doskonali jej kolejne części. Zakres realizowanych zadań jest dostosowany do etapu przygotowania pracy magisterskiej.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[KRYMMU2_U02] Potrafi samodzielnie zdobywać wiedzę i rozwijać kompetencje zawodowe, korzystając z różnych źródeł (w języku polskim i obcym) oraz nowoczesnych technologii.	Student potrafi samodzielnie pozyskiwać, selekcionować, krytycznie oceniać i wykorzystywać polskie i zagraniczne źródła naukowe, prawne i techniczne oraz posługiwać się nowoczesnymi narzędziami wspierającymi realizację badań i przygotowanie pracy magisterskiej.	[SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_U05] Posiada umiejętność samodzielnego proponowania rozwiązań problemów, przeprowadzania procesu podejmowania decyzji w tym zakresie, organizowania i koordynowania pracy zespołu oraz podejmowania działań w sposób przedsiębiorczy.	Student potrafi samodzielnie rozwiązywać problemy pojawiające się w toku przygotowania pracy magisterskiej, podejmować uzasadnione decyzje dotyczące metod, struktury i kierunku prowadzonych badań oraz organizować proces realizacji pracy.	[SU5] realizacja zadania problemowego
	[KRYMMU2_U01] Potrafi wykorzystywać wiedzę teoretyczną z zakresu kryminologii oraz nauk powiązanych do analizy, syntezy i interpretacji złożonych i nietypowych problemów oraz formułowania ich rozwiązań w zmiennych i nieprzewidywalnych warunkach.	Student potrafi wykorzystywać wiedzę z zakresu kryminologii, nauk prawnych i nauk pokrewnych do analizy, interpretacji i oceny złożonych problemów badawczych dotyczących cyberbezpieczeństwa, cyberprzestępczości i nowych technologii oraz formułować uzasadnione wnioski.	[SU2] prezentacja/projekt/referat/raport
	[KRYMMU2_K01] Ma świadomość poziomu swojej wiedzy i umiejętności, dokonuje ich krytycznej oceny, rozumie potrzebę uczenia się przez całe życie oraz uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych, a w przypadku trudności z samodzielnym rozwiązaniem problemu potrafi zasięgać opinii ekspertów.	Student potrafi krytycznie oceniać własną wiedzę i przygotowywane wyniki badań, identyfikować potrzebę pogłębienia wiedzy oraz wykorzystywać merytoryczną dyskusję i konsultacje w procesie przygotowania pracy magisterskiej.	[SK1] wypowiedź ustna/rozmowa/diskusja
	[KRYMMU2_K03] Jest przekonany o konieczności postępowania w sposób etyczny i profesjonalny, działa zgodnie z zasadami etyki, dostrzega i formułuje problemy moralne oraz dylematy etyczne związane z pracą własną i innych osób oraz poszukuje ich optymalnych rozwiązań.	Student stosuje zasady etyki i rzetelności naukowej w procesie przygotowania pracy magisterskiej, potrafi identyfikować problemy etyczne związane z prowadzeniem badań, korzystaniem ze źródeł oraz wykorzystywaniem narzędzi sztucznej inteligencji.	[SK1] wypowiedź ustna/rozmowa/diskusja
Treści przedmiotu	Problematyka seminarium koncentruje się na prawnych i kryminologicznych aspektach rozwoju technologii cyfrowych, w szczególności cyberbezpieczeństwie, cyberprzestępczości, ochronie praw podstawowych w środowisku cyfrowym oraz regulacji nowych i przełomowych technologii. W ramach zajęć omawiane są w szczególności: zasady wyboru problemu badawczego; formułowanie celu, pytań badawczych i tez pracy; metody badań właściwe dla nauk prawnych i kryminologii; wyszukiwanie, selekcja i krytyczna analiza literatury, aktów prawnych, orzecznictwa oraz innych materiałów źródłowych; korzystanie z krajowych, unijnych i międzynarodowych baz informacji prawnej i naukowej; konstruowanie struktury pracy; zasady argumentacji naukowej; opracowywanie i dyskusja kolejnych części pracy magisterskiej; zasady cytowania i dokumentowania źródeł; weryfikacja, redakcja i doskonalenie przygotowywanego tekstu oraz zasady rzetelności naukowej, w tym etycznego i zgodnego z obowiązującymi zasadami wykorzystania narzędzi sztucznej inteligencji. Przedmiotem dyskusji seminaryjnych są również aktualne problemy regulacyjne związane m.in. z krajowym i unijnym prawem cyberbezpieczeństwa, cyberprzestępczością, bezpieczeństwem produktów i usług cyfrowych, ochroną infrastruktury krytycznej, regulacją sztucznej inteligencji, automatyczną moderacją treści, mową nienawiści, inwigilacją elektroniczną, ochroną prywatności i danych, szyfrowaniem oraz rozwojem technologii przełomowych, w tym technologii kwantowych.		

Wymagania wstępne i dodatkowe	Podstawowa wiedza z zakresu kryminologii oraz podstaw prawa i funkcjonowania systemu prawnego. Umiejętność samodzielnego wyszukiwania i analizy literatury naukowej oraz materiałów źródłowych. Znajomość języka angielskiego umożliwiającą korzystanie z literatury naukowej, aktów prawa Unii Europejskiej i materiałów instytucji międzynarodowych jest zalecana. Nie jest wymagana specjalistyczna wiedza techniczna z zakresu informatyki lub cyberbezpieczeństwa; zakres niezbędnej wiedzy technicznej jest uzależniony od wybranego tematu pracy magisterskiej.		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Terminowa i zgodna z ustaleniami z promotorem realizacja kolejnych etapów przygotowania pracy magisterskiej, odpowiednio do stopnia zaawansowania prac	51.0%	100.0%
Zalecana lista lektur	Podstawowa lista lektur	1. C. Banasiński (red.), <i>Cyberbezpieczeństwo. Zarys wykładu</i> , wyd. 2, Wolters Kluwer, Warszawa 2023. 2. P. Opitek, D.R. Jaworski, <i>Cyberprzestępczość w prawie karnym i kryminalistyce. Kompendium wiedzy</i> , Difin, Warszawa 2025. 3. M.G. Porcedda, <i>Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis</i> , Hart Publishing, 2023. 4. A. Murray, <i>Information Technology Law: The Law and Society</i> , 5th ed., Oxford University Press, 2023. 5. V. Franssen, S. Tosza (red.), <i>The Cambridge Handbook of Digital Evidence in Criminal Investigations</i> , Cambridge University Press, 2025.	
	Uzupełniająca lista lektur	1. D.R. Jaworski (red.), <i>Cyberprzestępczość i nowe technologie. Współczesne wyzwania nauk prawnych</i> , Difin, Warszawa 2024. 2. M. Siwicki, <i>Cyberprzestępczość</i> , C.H. Beck, Warszawa 2013. 3. J. Stelmach, B. Brożek, <i>Metody prawnicze. Logika, analiza, argumentacja, hermeneutyka</i> , wyd. 2, Wolters Kluwer, Kraków 2006. 4. M. Rojszczak, <i>Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective</i> , Routledge, 2024. 5. M. Rojszczak, <i>Beyond Hate Speech: Clearly Unlawful Content in EU Digital Law</i> , Routledge, 2026. 6. P. Hacker, A. Engel, S. Hammer, B. Mittelstadt (red.), <i>The Oxford Handbook of the Foundations and Regulation of Generative AI</i> , Oxford University Press, 2026.	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Przykładowe obszary badawcze / tematy prac dyplomowych: 1. Europejski model regulacji cyberbezpieczeństwa po NIS2: spójny system czy fragmentaryzacja obowiązków regulacyjnych? 2. Odpowiedzialność producentów za cyberbezpieczeństwo produktów z elementami cyfrowymi w świetle Cyber Resilience Act. 3. Implementacja dyrektywy NIS2 w Polsce: ewolucja krajowego systemu cyberbezpieczeństwa i nowe obowiązki podmiotów kluczowych i ważnych. 4. Ransomware jako współczesna forma cyberprzestępczości - problemy odpowiedzialności karnej, ścigania i przeciwdziałania. 5. Elektroniczny materiał dowodowy w zwalczaniu cyberprzestępczości: europejski system e-Evidence a prawa jednostki. 6. Szyfrowanie end-to-end a zwalczanie poważnej przestępczości – granice prawnych obowiązków dostawców usług cyfrowych. 7. Automatyczne wykrywanie i usuwanie mowy nienawiści w usługach internetowych – pomiędzy zwalczaniem bezprawnych treści a wolnością wypowiedzi. 8. Sztuczna inteligencja w działaniach organów ścigania. Granice stosowania systemów predykcyjnych i analitycznych w świetle AI Act i praw podstawowych. 9. Cyberbezpieczeństwo systemów sztucznej inteligencji jako nowe wyzwanie regulacyjne (relacje AI Act, NIS2 i Cyber Resilience Act). 10. Rozwój komputerów kwantowych a prawna ochrona poufności komunikacji – czy prawo cyberbezpieczeństwa jest przygotowane na erę postkwantową? 11. Phishing, smishing i oszustwa wykorzystujące socjotechnikę jako formy cyberprzestępczości (problemy kwalifikacji prawnej, wykrywania i przeciwdziałania). 12. Złośliwe oprogramowanie, botnety i nieuprawniony dostęp do systemów informatycznych: odpowiedzialność karna oraz problemy ścigania sprawców cyberataków.		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.