Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Seminarium II - ROJSZCZAK Marcin, PG_00198669						
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	3		Liczba punktów ECTS	3.0			
Profil kształcenia	ogólnoakademicki		Forma zaliczenia	zaliczenie			
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji						
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	45.0		75
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_W06] Ma pogłębioną wiedzę oraz zna terminologię z zakresu psychologii, socjologii i nauk pokrewnych wykorzystywanych w kryminologii, a także rozumie związane z nimi fundamentalne dylematy współczesnej cywilizacji. Zna również podstawowe zasady ochrony własności intelektualnej i prawa autorskiego oraz uwarunkowania tworzenia i rozwoju różnych form przedsiębiorczości.	Student zna i rozumie interdyscyplinarne uwarunkowania badań nad cyberprzestępczością i nowymi technologiami, w tym ich aspekty społeczne i psychologiczne, oraz zna podstawowe zasady ochrony własności intelektualnej i prawa autorskiego istotne przy przygotowywaniu pracy magisterskiej.	[SW1] wypowiedź ustna/rozmowa/ dyskusja
	[KRYMMU2_W01] Ma pogłębioną wiedzę o charakterze nauk prawnych oraz nauk penalnych, ich miejscu w systemie nauk, wzajemnych relacjach oraz głównych kierunkach rozwoju, a także o ich powiązaniach z innymi dziedzinami nauki oraz aksjologicznych i społecznych uwarunkowaniach działalności związanej z przeciwdziałaniem przestępczości.	Student ma pogłębioną wiedzę o prawnych i kryminologicznych aspektach cyberbezpieczeństwa, cyberprzestępczości i regulacji nowych technologii oraz rozumie ich związki z naukami penalnymi i innymi dyscyplinami wykorzystywanymi w kryminologii.	[SW2] 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/ dyskusja
	[KRYMMU2_W02] Ma pogłębioną wiedzę o charakterze nauk przyrodniczych powiązanych ze studiowanym kierunkiem, ich miejscu w systemie nauk i wzajemnych relacjach	Student zna i rozumie podstawowe techniczne i naukowe uwarunkowania zjawisk analizowanych w pracy magisterskiej, w szczególności dotyczących funkcjonowania technologii cyfrowych, systemów informatycznych, sztucznej inteligencji i innych technologii istotnych dla wybranego problemu badawczego.	[SW2] prezentacja/projekt/referat/ raport

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 umożliwiająca 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 osiąganych 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.), *Cyberbezpieczeństwo. Zarys wykładu*, wyd. 2, Wolters Kluwer, Warszawa 2023. 2. P. Opitek, D.R. Jaworski, *Cyberprzestępczość w prawie karnym i kryminalistyce. Kompendium wiedzy*, Difin, Warszawa 2025. 3. M.G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*, Hart Publishing, 2023. 4. A. Murray, *Information Technology Law: The Law and Society*, 5th ed., Oxford University Press, 2023. 5. V. Franssen, S. Tosza (red.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025.
Uzupełniająca lista lektur	1. D.R. Jaworski (red.), *Cyberprzestępczość i nowe technologie. Współczesne wyzwania nauk prawnych*, Difin, Warszawa 2024. 2. M. Siwicki, *Cyberprzestępczość*, C.H. Beck, Warszawa 2013. 3. J. Stelmach, B. Brożek, *Metody prawnicze. Logika, analiza, argumentacja, hermeneutyka*, wyd. 2, Wolters Kluwer, Kraków 2006. 4. M. Rojszczak, *Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective*, Routledge, 2024. 5. M. Rojszczak, *Beyond Hate Speech: Clearly Unlawful Content in EU Digital Law*, Routledge, 2026. 6. P. Hacker, A. Engel, S. Hammer, B. Mittelstadt (red.), *The Oxford Handbook of the Foundations and Regulation of Generative AI*, 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.