

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberprzestępczość i cyberbezpieczeństwo - wykład, PG_00132852						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu			2027/2028		
Poziom kształcenia	II stopnia	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	2	Język wykładowy			polski		
Semestr studiów	3	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	Studenci poznają prawne, procesowe i techniczne aspekty przestępstw związanych z technologiami informatycznymi oraz zaznajamiają się z podstawowymi zasadami i mechanizmami bezpieczeństwa systemów informatycznych, jak i z normami prawnymi regulującymi korzystanie z komputerów itp. i sieci teleinformatycznych.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[KRYMMU2_W01] Ma pogłębioną wiedzę o charakterze nauk prawnych oraz nauk penalnych, ich miejscu w systemie nauk, wzajemnych relacjach oraz głównych kierunkach ich rozwoju.	Student zna niebezpieczeństwa związane z użytkowaniem komputerów i sieci informatycznych, zasady zarządzania bezpieczeństwem systemów informatycznych, niebezpieczeństwa dotyczące utraty prywatności, zasady ochrony własności intelektualnej oraz podstawy prawa patentowego i autorskiego.	[SW4] test/egzamin - ustny lub pisemny [SW1] wypowiedź ustna/rozmowa/dyskusja [SW5] realizacja zadania problemowego
	[KRYMMU2_W05] Ma pogłębioną wiedzę o metodach i narzędziach badawczych, w tym technikach pozyskiwania, analizy i interpretacji danych, właściwych dla kryminologii i kryminalistyki.	Student zna niebezpieczeństwa związane z użytkowaniem komputerów i sieci informatycznych, zasady zarządzania bezpieczeństwem systemów informatycznych, niebezpieczeństwa dotyczące utraty prywatności, zasady ochrony własności intelektualnej oraz podstawy prawa patentowego i autorskiego.	[SW4] test/egzamin - ustny lub pisemny [SW1] wypowiedź ustna/rozmowa/dyskusja [SW5] realizacja zadania problemowego
[KRYMMU2_K05] Potrafi samodzielnie i krytycznie rozwijać swoją wiedzę i umiejętności, z uwzględnieniem ich interdyscyplinarnego charakteru.	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SK1] wypowiedź ustna/rozmowa/dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego	
Treści przedmiotu	<p>1. Identyfikacja komputera w sieci: adresy MAC, IP (statyczne, dynamiczne; prywatne, publiczne), whois domenowe, sieciowe, DHCP, NAT, porty, ISP, ICP, IAP, domena (subdomena), hosting, usługi chmurowe, rola serwerów DNS, identyfikacja operatora.</p> <p>2. Rozliczalność działań w sieci Internet: anonimizacja połączeń, Proxy, VPN, sieć TOR, Darknet, anonimizacja poczty elektronicznej</p> <p>3. Identyfikacja znamion przestępstw komputerowych. Przykłady narzędzi i metod cyberprzestępców: identity theft, spoofing, hasła i statyczne dane dostępowe, phishing, man-in-the-middle, spam, whaling (CEO Fraud), dezinformacja, fake news, SQL/HTML Injection, formjacking, exploit kits, darknet i blockchain</p>		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	test	51.0%	100.0%
Zalecana lista lektur	Podstawowa lista lektur	<p>J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015</p> <p>C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo wyd. 2, WoltersKluwer, Warszawa 2023</p> <p>F.Wołowski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012</p>	

	Uzupełniająca lista lektur	<p>K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2021</p> <p>M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securitum 2024</p> <p>M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 2, Securitum 2025</p> <p>D. Lisiak-Felicka, M. Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, IASF, Kraków 2016, ss. 222; https://www.netcomplex.pl/blog/wp-content/uploads/2016/04/Cyberbezpieczenstwo_Lisiak_Felicka__Szmit.pdf</p> <p>D. Siemieniecka, M. Skibińska, K. Majewska, Cyberagresja zjawisko, skutki, zapobieganie, UMK 2020, ss. 198; https://wydawnictwo.umk.pl/pl/products/5275/cyberagresja-zjawisko-skutki-zapobieganie</p> <p>M. Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, Wyd. II, PTI, Warszawa 2014; ss. 238; https://historiainformatyki.pl/historia/dokument.php?nonav=&nrrar=6&nrzesp=6&sygn=V%2F1%2F7&handle=1&folder=1</p> <p>J. Wasilewski, Cyberprzestępczość wybrane aspekty prawnokarne oraz kryminalistyczne, Uniw. w Białymstoku, Białystok 2018, ss. 429; https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf</p> <p>Białas Andrzej, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2007</p> <p>PN-I-13335:1999, Wytoczne do zarządzania bezpieczeństwem systemów informatycznych</p>
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.