Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberprzestępczość i cyberbezpieczeństwo - ćwiczenia , PG_00132526						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2025 r.		Rok akademicki realizacji przedmiotu	2026/2027			
Poziom kształcenia	II stopnia		Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów			
Forma studiów	niestacjonarne		Sposób realizacji	na uczelni			
Rok studiów	2		Język wykładowy	polski			
Semestr studiów	3		Liczba punktów ECTS	1.0			
Profil kształcenia	ogólnoakademicki		Forma zaliczenia	zaliczenie			
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji -> Katedra Informatyki Prawniczej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	mgr Patryk Ciurak					
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	0.0	10.0	0.0	0.0	0.0	10
	W tym liczba godzin zajęć na odległość: 0.0						
	Dodatkowe informacje: Dyskusja Analiza zdarzeń krytycznych (przypadków) Praca w grupach						
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	10	0.0	15.0	25		
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_UW05] Posiada umiejętność samodzielnego proponowania rozwiązań konkretnego problemu i przeprowadzenia procedury podjęcia rozstrzygnięć w tym zakresie	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.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
[KRYMMU2_UW02] Potrafi samodzielnie zdobywać wiedzę i rozwijać swoje profesjonalne umiejętności, korzystając z różnych źródeł (w języku rodzimym i obcym) i nowoczesnych technologii	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.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
[KRYMMU2_K05] Potrafi samodzielnie i krytycznie uzupełniać wiedzę i umiejętności, rozszerzone o wymiar interdyscyplinarny	Student nie nadużywa systemów informatycznych naruszając cudzą prywatność, nie dokonuje czynów zabronionych ani nieetycznych związanych z użytkowaniem komputerów i sieci informatycznych, nie używa oprogramowania, do którego nie nabył prawa.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta
[KRYMMU2_UW01] Potrafi wykorzystywać wiedzę teoretyczną z zakresu kryminologii oraz powiązanych z nią dyscyplin naukowych w celu analizowania i interpretowania problemów związanych z kryminologią szeroko rozumianą	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.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta

Treści przedmiotu

Cyberhigiena i rozliczalność działań w sieci
Kradzież tożsamości
Spoofing
Phishing
Man-in-the-Middle
HTML/SQL Injection, formjacking
Botnet, DDoS
Dezinformacja, fakenews
Socjotechnika
OSINT
Analiza ryzyka

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Kolokwium	51.0%	100.0%

Zalecana lista lektur

Podstawowa lista lektur

J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015

C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo wyd. 2, WoltersKluwer, Warszawa 2023

Wprowadzenie do bezpieczeństwa IT, t. 1, red. M. Sajdak, Securitum (Kraków) 2024

Wprowadzenie do bezpieczeństwa IT, t. 2, red. M. Sajdak, Securitum (Kraków) 2025

	Uzupełniająca lista lektur	F.Wołowski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012 K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2022 M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securitum 2023 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 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 M.Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, Wyd. II, PTI, Warszawa 2014; ss. 238; https://historiainformatyki.pl/historia/dokument.php?nonav=&nrar=6&nrzesp=6&sygn=V%2F1%2F7&handle=1&folder=1 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 Białas Andrzej, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2007 PN-I-13335:1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych
	Adresy eZasobów	Adresy na platformie eNauczanie:
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.