Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberprzemoc - wykład, PG_00131736						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2023 r.		Rok akademicki realizacji przedmiotu	2024/2025			
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć	Grupa zajęć fakultatywnych			
Forma studiów	stacjonarne		Sposób realizacji	na uczelni			
Rok studiów	2		Język wykładowy	polski			
Semestr studiów	4		Liczba punktów ECTS	1.0			
Profil kształcenia	ogólnoakademicki		Forma zaliczenia	zaliczenie			
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr Mateusz Lammek					
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	20.0	0.0	0.0	0.0	0.0	20
	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	20		0.0	5.0		25
Cel przedmiotu	Zajęcia mają na celu wyposażyć studentów w podstawową wiedzę na temat cyberprzestępczości. Student potrafi wymienić formy przestępstw z użyciem komputera oraz innych nowych technologii, jest świadomy nowych problemów związanych z cyberprzestępczością oraz posiada podstawową wiedzę na temat mechanizmów psychologicznych dokonywania przestępstw jak i form zabezpieczeń przeciwko takim działaniom.						

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[KRYML3_KK01] Ma świadomość poziomu swojej wiedzy i umiejętności, a także rozumie potrzebę uczenia się przez całe życie.	Student wyróżnia typy cyberprzestępczości, zna podstawowe zabezpieczenia sieci i komputera. Posiada informacje nt. mechanizmów psychologicznych, które wpływają na dokonywanie przestępstw przy użyciu komputera.	[SK1] wypowiedź ustna/rozmowa/ dyskusja
[KRYML3_UU02] Potrafi wykorzystywać podstawową wiedzę teoretyczną z zakresu kryminologii oraz powiązanych z nią dyscyplin naukowych w celu analizowania, interpretowania i rozwiązywania problemów związanych z kryminologią.	Zajęcia mają na celu wyposażyć studentów w podstawową wiedzę na temat cyberprzestępczości. Student potrafi wymienić formy przestępstw z użyciem komputera oraz innych nowych technologii, jest świadomy nowych problemów związanych z cyberprzestępczością oraz posiada podstawową wiedzę na temat zabezpieczeń.	[SU4] test/egzamin - ustny lub pisemny
[KRYML3_WG01] Ma elementarną wiedzę o charakterze nauk prawnych oraz związanych z naukami o przestępstwie, ich miejscu w systemie nauk i wzajemnych relacjach.	Student potrafi zdefiniować cyberprzestępczość. Posiada postawowe informacje związane z ukrytą siecią. Wie, jakie przestępstwa z użyciem komputera zostały ujęte w Kodeksie Karnym. Posiada wiedzę na temat istniejących zabezpieczeń sieci i komputera. Potrafi wskazać mechanizmy psychologiczne, które wpływają na dokonywanie e-przestępstw. Posiada informacje dotyczące możliwości Policji w ściganiu cyberprzestępczości, potrafi wskazać obszar pracy dla psychologa.	[SW1] wypowiedź ustna/rozmowa/ dyskusja
[KRYML3_WG02] Zna podstawową terminologię oraz podstawowe pojęcia z zakresu prawa, kryminologii oraz nauk z nimi powiązanych.	Student aktywnie uczestniczy w ćwiczeniach. Uczy się wypowiadania własnego zdania, bez krytyki innego punktu widzenia. Potrafi generować pomysły dotyczące nowych zadań dla psychologa w odniesieniu do nowych problemów związanych z cyberprzestępczością.	[SW5] realizacja zadania problemowego

Treści przedmiotu

Możliwości wykorzystywania Internetu (nie tylko legalne), pojęcie cyberprzestępstwa w ujęciu prawnym, podział przestępstw z użyciem komputera w Kodeksie Karnym
Ukryta sieć (deep web) jak działa, jak korzystać, jakie są możliwości i zagrożenia użytkowania
Nowe formy przestępstw: hacking, nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych, niszczenie/ usuwanie/ modyfikowanie danych informatycznych, sabotaż komputerowy, zakłócenie pracy systemu lub sieci, wytwarzanie i/lub udostępnianie programów przystosowanych do popełnienia przestępstwa
Przestępstwa związane z e-bankowością. Kto najczęściej zostaje ofiarą tego typu przestępstw? Jak można się bronić?
Przestępstwa przeciwko życiu w Internecie filmy snuff, oferty płatnych zabójców itp. Seks z Internecie gwałty, handel ludźmi, pedofilia, pornografia dostępność i popularność materiałów
Zniekształcenia poznawcze związane z dokonywaniem przestępstw w Internecie, świadomość prawna młodzieży, e-środowisko a postępująca psychopatyzacja społeczeństwa
Bezpieczeństwo w sieci. Jak można chronić dane wrażliwe? Czy można zapobiegać internetowym przestępstwom? Jak reagować na oszustwa w Internecie? nasze prawa oraz obowiązki. E-przestępstwa a możliwości działania Policji. Psycholog i nowe wyzwania związane z cyberprzestępczością.

Wymagania wstępne i dodatkowe

Podstawowa wiedza dotycząca norm prawnych oraz nowych technologii

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
zadania problemowe	51.0%	20.0%
test	51.0%	80.0%

Zalecana lista lektur

Podstawowa lista lektur

Kosiński J., (2015) Paradygmaty cyberprzestępczości, Warszawa: Difin
Marczak M., Pastwa Wojciechowska B., Błażek M. (2010), Wiedza, doświadczenie, praktyka: interdyscyplinarne spojrzenie na problemy społeczne, Gdańsk: Uniwersytet Gdański
Pastwa Wojciechowska B. (2008). Człowiek w obliczu prawa, Kraków: Impuls
Shinder D. L. (2004), Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci, Gliwice: Helion
Siwicki M., (2013), Cyberprzestępczość, Warszawa: Wydawnictwo C.H. Beck
Szpor G., Gryszczyńska A., (2017). Internet. Strategie bezpieczeństwa. Warszawa: C.H.Beck

	Uzupełniająca lista lektur	Opitek P., (2017), Skimming: aspekty kryminalistyczne, cyberprzestępczość w bankowości elektronicznej, Warszawa: Wydawnictwo C. H. Beck Grzelak, M., & Liedel, K. (2014). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polskizarys problemu. Zeszyty Naukowe Uniwersytetu Ekonomicznego. Kraków, Wydawnictwo UE, (2), 926.
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Możliwości wykorzystywania Internetu (nie tylko legalne), pojęcie cyberprzestępstwa w ujęciu prawnym, podział przestępstw z użyciem komputera w Kodeksie Karnym Ukryta sieć (deep web) jak działa, jak korzystać, jakie są możliwości i zagrożenia użytkowania Nowe formy przestępstw: hacking, nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych, niszczenie/ usuwanie/ modyfikowanie danych informatycznych, sabotaż komputerowy, zakłócenie pracy systemu lub sieci, wytwarzanie i/lub udostępnianie programów przystosowanych do popełnienia przestępstwa Przestępstwa związane z e-bankowością. Kto najczęściej zostaje ofiarą tego typu przestępstw? Jak można się bronić? Przestępstwa przeciwko życiu w Internecie filmy snuff, oferty płatnych zabójców itp. Seks z Internecie gwałty, handel ludźmi, pedofilia, pornografia dostępność i popularność materiałów Zniekształcenia poznawcze związane z dokonywaniem przestępstw w Internecie, świadomość prawna młodzieży, e-środowisko a postępująca psychopatyzacja społeczeństwa Bezpieczeństwo w sieci. Jak można chronić dane wrażliwe? Czy można zapobiegać internetowym przestępstwom? Jak reagować na oszustwa w Internecie? nasze prawa oraz obowiązki. E-przestępstwa a możliwości działania Policji. Psycholog i nowe wyzwania związane z cyberprzestępczością.	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.