Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo - wykład, PG_00131767						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu	2026/2027			
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów			
Forma studiów	stacjonarne		Sposób realizacji	na uczelni			
Rok studiów	3		Język wykładowy	polski			
Semestr studiów	6		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						
	Adres kursu na platformie eNauczanie: https://mdl.ug.edu.pl/course/view.php?id=12893						
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	Uzyskanie wiedzy i umiejętności niezbędnych do opracowania projektów i strategii ograniczania ryzyka cybernetycznego, w tym odpowiednich kroków prawnych, które należy podjąć w odpowiedzi na ataki cybernetyczne. Dogłębne zrozumienie różnych rodzajów ataków cybernetycznych, na które są narażone systemy informacyjne biznesu i administracji. Poznanie roli i znaczenia podejścia do bezpieczeństwa cybernetycznego w całej organizacji opartego na ocenie ryzyka.						

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[KRYML3_UW01] Potrafi dokonać obserwacji i interpretacji zjawisk społecznych, analizuje ich powiązania z różnymi obszarami działalności kryminologii.	Student: 1. Zna podstawowe sposoby zapobiegania atakom na systemy informacyjne, zwalczania takich ataków, zabezpieczania dowodów i raportowania incydentów bezpieczeństwa. 2. Umie wykonać analizę ryzyka systemy, stanowiska roboczego, organizacji i procesu. 3. Umie analizować i rozumie informacje związanych z obowiązkami nałożonymi na najważniejszych aktorów funkcjonujących w obszarze cyberbezpieczeństwa. 4. Potrafi stosować w praktyce mechanizmy działania krajowego systemu cyberbezpieczeństwa.	[SU3] opracowanie tekstowe/ praca pisemna [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego
[KRYML3_KK01] Ma świadomość poziomu swojej wiedzy i umiejętności, a także rozumie potrzebę uczenia się przez całe życie.	Student: 1. Zachowuje podstawowe zasady cyberhigieny w środowsku pracy i w miejscu zamieszkania. 2. Potrafi służyć poradą w kwestiach bezpieczeństwa informacyjnego. 3. Rozumie skomplikowane, interdyscyplinarne zależności związane ze funkcjonowaniem krajowego systemu cyberbezpieczeństwa.	[SK3] opracowanie tekstowe/ praca pisemna [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego
[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.	Student. 1. Zna obowiązki i uprawnienia podmiotów państwowych i prywatnych wynikające z wykorzystywania nowych technologii informacyjnych i komunikacyjnych. 2. Wie jaki działania należy podejmować ograniczając zagrożenia pochodzące z cyberprzestrzeni.	[SU3] opracowanie tekstowe/ praca pisemna [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego

Treści przedmiotu

1. Podstawowe pojęcia związane z cyberbezpieczeństwem.
2. Cyberprzestrzeń a Internet
3. Prawne modele regulacji cyberprzestrzeni
4. Regulacja Internetu
5. Sieci komputerowe i podstawowe kategorie cyberprzestępstw
6. Unijny system cyberbezpieczeństwa. Ramy prawne
7. Cyberhigiena

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Pisemne rozwiązanie zagadnienia problemowego	51.0%	100.0%

Zalecana lista lektur

Podstawowa lista lektur	1. C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu, wyd. 2. Wolters Kluwer, Warszawa 2023 2. K. Czaplicki, A. Gryszczyńska, G. Szpor [red.:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, Warszawa 2019
Uzupełniająca lista lektur	1. F. Wołowski, J. Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków 2012; 2. J. Łuczak, M. Tyburski, Systemowe zarządzanie bezpieczestwem informacji wg ISO/IEC 27001:2005, Wyd. UE, Poznań 2009; 3. K. Liderman, Bezpieczeństwo informacyjne : nowe wyzwania, Warszawa, 2017 4. D. Szostek [red.:] Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/adwokackiej/notarialnej/ komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej C.H.Beck, Warszawa 2018; 5. D. Lisiak-Felicka, M. Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, European Association For Security, Kraków 2016, https://www.researchgate.net/ publication/ 301204372_Cyberbezpieczenstwo_administracji_publicznej_w_Pols 570c7d4d08ae2eb94223c4f7/download 6. M. Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, European Association For Security, Kraków 2014; 7. N. Polemi, Port Cybersecurity. Securing critical information ifrastructures and supply chains, Elsevier, Amsterdam-Oksford-Cambridge 2018; 8. J. Kossoff, Cybersecurity Law, Wiley, Hoboken 2020.
Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.