Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Prawo cyberbezpieczeństwa i infrastruktury informatycznej - ćwiczenia, PG_00198183		
Kierunek studiów	Administracja (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	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	15.0	0.0	0.0	0.0	15

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	15	2.0	8.0	25

Cel przedmiotu

Celem ćwiczeń jest przygotowanie w podstawowym zakresie do stosowania regulacji (zarówno prawa stanowionego jak i soft-law) dotyczących cyberbezpieczeństwa, w tym ochrony infrastruktury informatycznej, a także komunikacji w tym zakresie.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[ADMINMU2_W03] zna i rozumie aktualne dylematy dotyczące funkcjonowania administracji oraz stosowania w sferze państwa, administracji oraz gospodarki instytucji prawa, w tym w kontekście tworzenia i rozwoju różnych form przedsiębiorczości, z szczególnym uwzględnieniem regulacji prawa nowych technologii	Student rozumie funkcje cyberbezpieczeństwa i ochrony infrastruktury informatycznej w społeczeństwie w kontekście rozwoju cywilizacyjnego.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW3] opracowanie tekstowe/ praca pisemna
[ADMINMU2_U02] w pogłębionym stopniu potrafi komunikować się w kwestiach związanych z problemami prawnymi i organizacyjnymi w pracy zawodowej – zarówno ustnie jak i na piśmie, a także jest zdolny do formułowania zrozumiałego przekazu osobom będącym i nie będącym specjalistami w administracji	Student potrafi komunikować się z innymi w kwestii zdarzeń związanych z cyberbezpieczeństwem i ochroną infrastruktury informatycznej.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
[ADMINMU2_U01] wykorzystując własną wiedzę oraz inne źródła informacji potrafi identyfikować, analizować i rozstrzygać złożone problemy i formułować własne tezy, a także interpretować zjawiska dotyczące organizacji i funkcjonowania administracji oraz wybranych domen życia społecznego i gospodarczego, w szczególności charakterystycznych dla państwa i społeczeństwa informacyjnego	Student potrafi identyfikować sytuacje naruszenia bezpieczeństwa danych lub infrastruktury informatycznej.	[SU3] opracowanie tekstowe/ praca pisemna [SU4] test/egzamin - ustny lub pisemny

Treści przedmiotu

1. Podstawowe pojęcia związane z cyberbezpieczeństwem.

2. Modele regulacji i systemy cyberbezpieczeństwa

3. Sieci komputerowe i podstawowe kategorie cyberprzestępstw

4. Cyberhigiena i inne praktyki z zakresu cyberbezpieczeństwa.

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

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

Zalecana lista lektur

Podstawowa lista lektur	Studenci korzystają z aktów normatywnych regulujących zagadnienia objęte programem. C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo, Warszawa (aktualne wydanie) M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securitum 2024 M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 2, Securitum 2025

	Uzupełniająca lista lektur	C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa (aktualne wydanie). J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015 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.